Cisco Security Manager 4.4 ハイ アベイラビリティ インストレーション ガイド

2013 年 2 月

Text Part Number: OL-28925-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco Security Manager 4.4 ハイ アベイラビリティ インストレーション ガイド
© 2007-2013 Cisco Systems, Inc. All rights reserved.

Text Part Number: OL-28925-01-J

CONTENTS

はじめに vii

対象読者 vii

表記法 viii

関連資料 ix

マニュアルの入手方法およびテクニカル サポート x

CHAPTER 1 概要 1-1

ローカル冗長性（HA）プロセスの概要 1-1

ローカル冗長性（HA）の設定手順 1-2

地理的冗長性（DR）プロセスの概要 1-3

地理的冗長性（DR）の設定手順 1-4

Symantec Veritas 製品 1-5

CHAPTER 2 システム要件 2-1

シングル ノード サイトのハードウェア要件 2-1

デュアル ノード サイトのハードウェア要件 2-2

ローカル冗長性構成のソフトウェア要件 2-3

地理的冗長性（DR）構成のソフトウェア要件 2-4

クラスタリングが不要な複製のソフトウェア要件 2-4

プリインストール ワークシート 2-5

ローカル冗長性構成のワークシート 2-5

地理的冗長性（DR）設定ワークシート 2-6

CHAPTER 3 Cisco Security Management Suite ハイ アベイラビリティ ソリューションのインストール 3-1

イーサネット接続の確立 3-1

Microsoft Windows Server のインストール 3-2

外部ストレージへのサーバの接続 3-2

Symantec Veritas 製品のインストール 3-2

ブート ディスクのミラーリング（任意） 3-3

Veritas Volume Manager の設定タスク 3-4

プライマリ サーバ（複製なし） 3-4

プライマリ サーバ（複製あり） 3-5

セカンダリ サーバとセカンダリ クラスタ内のプライマリ サーバ 3-6
Security Manager のインストール 3-6
プライマリ サーバへの Security Manager のインストール 3-7
セカンダリ サーバへの Security Manager のインストール 3-9
Veritas Volume Replicator タスク 3-12
作業ボリュームに対する権限の更新 3-14
共有ストレージを使用する場合の権限の更新 3-14
複製を使用する場合の権限の更新 3-15
Veritas Cluster Server タスク 3-16
シングル ローカル クラスタ（デュアル ノード）構成 3-16
クラスタの作成 3-17
アプリケーション サービス グループの作成 3-17
ClusterService グループの作成（任意） 3-24
デュアル地理的クラスタ構成 3-25
プライマリおよびセカンダリ クラスタの作成 3-25
ClusterService グループの作成 3-26
複製サービス グループの作成 3-27
アプリケーション サービス グループの作成 3-28
クラスタ レベル設定の作成 3-30

CHAPTER 4 メンテナンス作業 4-1
VCS 動作のカスタマイズ 4-1
SSL 用のセキュリティ証明書 4-2
Security Manager の手動での起動、停止、またはフェールオーバー 4-3
VCS の場合 4-3
VCS 以外の場合 4-4
Cisco Secure ACS と Security Manager の統合 4-6
Security Manager のアップグレード 4-6
Security Manager のバックアップ 4-7
Security Manager のアンインストール 4-7
HA への非 HA Security Manager の移行 4-8

APPENDIX A 参照構成の VCS リソース ビュー A-1
シングル ローカル クラスタ（デュアル ノード）構成 A-2
デュアル地理的クラスタ（シングル ノード）構成 A-3

APPENDIX B ハイ アベイラビリティおよびディザスタ リカバリ証明テスト計画 B-1
手動切り替え B-1

クラスタ内切り替え B-1
クラスタ間切り替え B-2
イーサネット / ネットワーク障害 B-3
ネットワーク通信障害 B-3
セカンダリ サーバ、シングル クラスタにおけるネットワーク イーサネット障害 B-3
プライマリ サーバ、シングル クラスタにおけるネットワーク イーサネット障害 B-4
セカンダリ サーバ、デュアル クラスタにおけるネットワーク イーサネット障害 B-5
プライマリ サーバ、デュアル クラスタにおけるネットワーク イーサネット障害 B-7
クラスタ通信障害 B-8
サーバの障害 B-10
スタンバイ サーバの障害、シングル クラスタ B-10
プライマリ サーバの障害、シングル クラスタ B-11
スタンバイ サーバの障害、デュアル クラスタ B-12
プライマリ サーバの障害、デュアル クラスタ B-14
アプリケーションの障害 B-16
アプリケーションの障害、シングル クラスタ B-16
アプリケーションの障害、デュアル クラスタ B-17

INDEX

はじめに

このマニュアルでは、ハイ アベイラビリティ（HA）環境やディザスタ リカバリ（DR）環境に Cisco Security Management Suite（Security Manager）をインストールする方法について説明します。Security Manager HA/DR ソリューションは、Symantec の Veritas Storage Foundation and High Availability Solutions に基づいています。

対象読者

このマニュアルの主な対象読者は、HA/DR ソリューションのインストールおよび管理を担当するシステム管理者です。このマニュアルでは、表 1 の内容をよく理解していることを前提としています。

表 1　　このマニュアルの内容

設定	内容
ローカル冗長性	• Cisco Security Management Suite • Microsoft Windows Administration（Microsoft Windows Server 2008 R2 Service Pack 1（64 ビット）Enterprise Edition または Microsoft Windows Server 2008 Service Pack 2（64 ビット）Enterprise Edition） • Symantec Veritas Storage Foundation HA for Windows 5.1 SP1 または 6.0

表 1　　このマニュアルの内容 （続き）

設定	内容
地理的冗長性	• Cisco Security Management Suite • Microsoft Windows Administration（Microsoft Windows Server 2008 R2 Service Pack 1（64 ビット）Enterprise Edition または Microsoft Windows Server 2008 Service Pack 2（64 ビット）Enterprise Edition） • Symantec Veritas Storage Foundation HA/DR for Windows 5.1 SP1 • Symantec Veritas Volume Replicator Option
地理的冗長性（クラスタリングなし）	• Cisco Security Management Suite • Microsoft Windows Administration（Microsoft Windows Server 2008 R2 Service Pack 1（64 ビット）Enterprise Edition または Microsoft Windows Server 2008 Service Pack 2（64 ビット）Enterprise Edition） • Symantec Veritas Storage Foundation Basic for Windows 5.1 SP1 • Symantec Veritas Volume Replicator Option

Security Manager HA/DR ソリューションは Symantec の Veritas Storage Foundation and High Availability Solutions for Windows を利用するため、ローカル冗長性ソリューションに関する次の Symantec コースを推奨します。

- Veritas Storage Foundation for Windows
- Veritas Cluster Server for Windows

地理的冗長性については、次のコースを受講することを強く推奨します。

- Veritas Volume Replicator for Windows
- Disaster Recovery Using Veritas Volume Replicator and Global Cluster Option for Windows

詳細については、Symantec の Web サイトを参照してください。

表記法

このマニュアルでは、次の表記法を使用しています。

項目	表記法
手順で選択する必要があるコマンド、キーワード、特殊な用語、およびオプション	**太字**フォント
ユーザが値を指定する変数、および新しい用語や重要な用語	*イタリック体*フォント
セッション情報、システム情報、パス、およびファイル名の表示出力	`screen` フォント
ユーザが入力する情報	**太字の screen** フォント
ユーザが入力する変数	*イタリック体の screen* フォント
メニュー項目の選択順序	[Option] > [Network Preferences]

ヒント 製品を最大限に活用できる情報を示します。

（注） 「*注釈*」です。次に進む前に検討する必要がある重要情報、役に立つ情報、このマニュアル以外の参照資料などを紹介しています。

注意 「*要注意*」の意味です。機器の損傷、データの損失、またはネットワーク セキュリティの侵害を予防するための注意事項が記述されています。

警告 **ユーザの身体、ソフトウェアの状態、または機器に被害が及ぶのを防ぐために、留意する必要がある注意事項が記述されています。記載された注意事項に従わない場合に、結果として発生するセキュリティ侵害が明確に特定されています。**

関連資料

追加情報については、次のシスコの資料を参照してください。これらの資料は、http://www.cisco.com/en/US/products/ps6498/tsd_products_support_series_home.html から入手できます。

- *『Installation Guide for Cisco Security Manager 4.4』*
- *『User Guide for Cisco Security Manager 4.4』*
- *『Release Notes for Cisco Security Manager 4.4』*

Veritas Storage Foundation に関連する詳細情報については、次の Symantec の資料を参照してください。

- *『Veritas Storage Foundation™ and High Availability Solutions Getting Started Guide』*
- *『Veritas Storage Foundation™ and High Availability Solutions Release Notes』*
- *『Veritas Storage Foundation™ and High Availability Solutions Installation and Upgrade Guide』*
- *『Veritas Storage Foundation™ Administrator's Guide』*
- *『Veritas™ Cluster Server Release Notes』*
- *『Veritas™ Cluster Server Installation and Upgrade Guide』*
- *『Veritas™ Cluster Server Bundled Agents Reference Guide』*
- *『Veritas™ Cluster Server Administrator's Guide』*
- *『Veritas™ Volume Replicator Administrator's Guide』*
- *『Veritas™ Volume Replicator Advisor User's Guide』*
- *『Hardware Compatibility List (HCL) for Veritas Storage Foundation™ and High Availability Solutions for Windows』*
- *『Software Compatibility List (SCL) for Veritas Storage Foundation™ and High Availability Solutions for Windows』*

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 1

概要

このマニュアルでは、ハイ アベイラビリティ（HA）環境やディザスタ リカバリ（DR）環境に Cisco Security Management Suite（Security Manager）をインストールする方法について説明します。Security Manager HA/DR ソリューションは、Symantec の Veritas Storage Foundation and High Availability Solutions に基づいています。このマニュアルで説明する Security Manager HA/DR ソリューションは次のアプリケーションをサポートしています。

- Security Manager 4.4
- Auto Update Server（AUS）4.4

（注） デバイスは AUS サーバ IP アドレスを直接使用して AUS サーバに接続するため、デバイスが各サイトの AUS サーバの IP アドレスが異なる DR 構成において最大 2 台の AUS サーバの定義をサポートする必要があります。複数の AUS サーバ IP アドレスの定義は、リリース 7.2.1 以降の ASA 5500 シリーズだけでサポートされます。

HA ソリューションは、ローカル冗長性（HA）と地理的冗長性（DR）の両方の構成をサポートします。

ここでは、次の概要を示します。

- 「ローカル冗長性（HA）プロセスの概要」（P.1-1）
- 「地理的冗長性（DR）プロセスの概要」（P.1-3）
- 「Symantec Veritas 製品」（P.1-5）

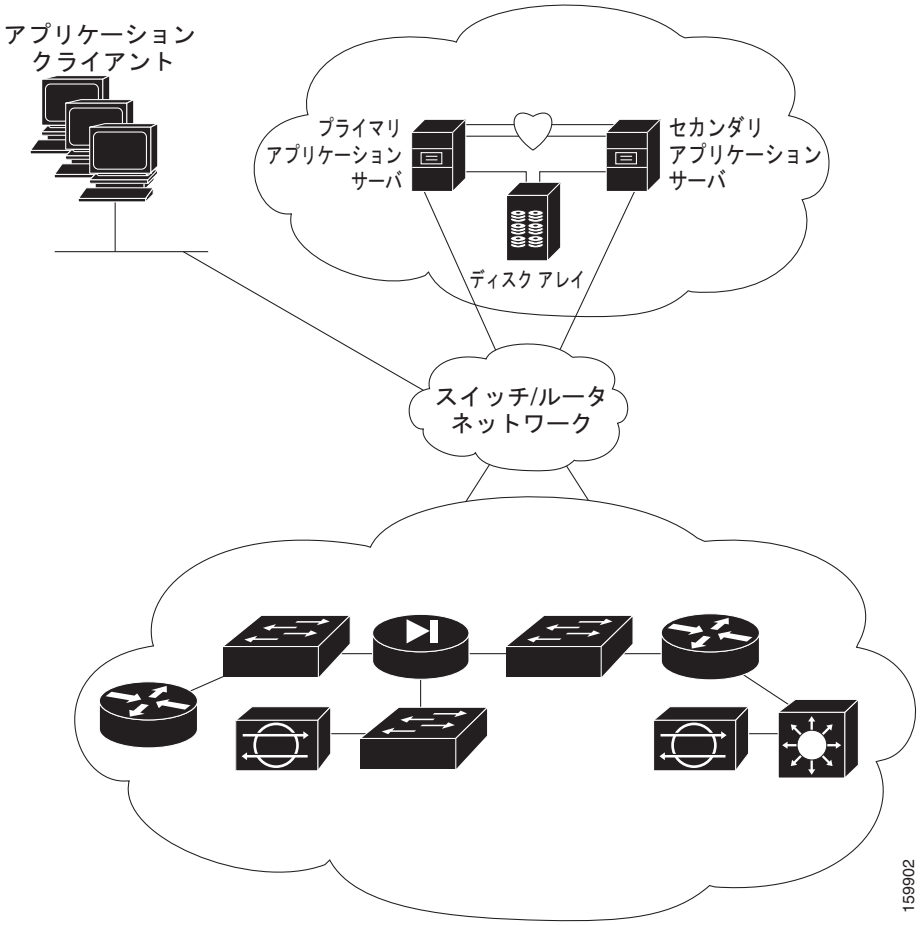
ローカル冗長性（HA）プロセスの概要

ローカル冗長性の構成は、ソフトウェアまたはハードウェア障害の際にも、スイッチド ネットワークおよびルーテッド ネットワークで IP アドレスや DNS エントリを再設定する必要がない、自動フェールオーバー ソリューションを提供します。

図 1-1 に、ローカル冗長性 HA の構成を示します。

（注） 図 1-1 のサーバには、ミラーリングされた内蔵ブート ディスクが含まれることがあります。同じメーカー、モデル、およびストレージ容量にすることを推奨します。HA サーバとの通信にはフォールトトレラントなスイッチド/ルーテッド ネットワークを推奨します。

図 1-1　ローカル冗長性 HA の構成



ローカル冗長性（HA）の設定手順

次の表に、Cisco Security Manager のローカルな冗長性を持つインストールを設定するために必要な手順を示します。

	タスク	参照
ステップ 1	物理接続を確立します。	「イーサネット接続の確立」（P.3-1）
ステップ 2	Microsoft Windows サーバとすべての必要なドライバをインストールします。	「Microsoft Windows Server のインストール」（P.3-2）
ステップ 3	ストレージ接続を確立します。	「外部ストレージへのサーバの接続」（P.3-2）
ステップ 4	Symantec Veritas 製品およびコンポーネントをインストールして設定します。	「Symantec Veritas 製品のインストール」（P.3-2）
ステップ 5	ブート ディスクをミラーリングします。	「ブート ディスクのミラーリング（任意）」（P.3-3）

	タスク	参照
ステップ 6	共有アレイに必要なボリュームをセットアップします。	「Veritas Volume Manager の設定タスク」（P.3-4）
ステップ 7	プライマリ サーバの共有ボリューム上に Cisco Security Manager をインストールします。	「Security Manager のインストール」（P.3-6）
ステップ 8	セカンダリ サーバのスペア（ダミー）ボリューム上に Cisco Security Manager をインストールします。	「Security Manager のインストール」（P.3-6）
ステップ 9	セカンダリ サーバに対する権限を更新します。	「作業ボリュームに対する権限の更新」（P.3-14）
ステップ 10	クラスタを作成し、設定します。	「Veritas Cluster Server タスク」（P.3-16）

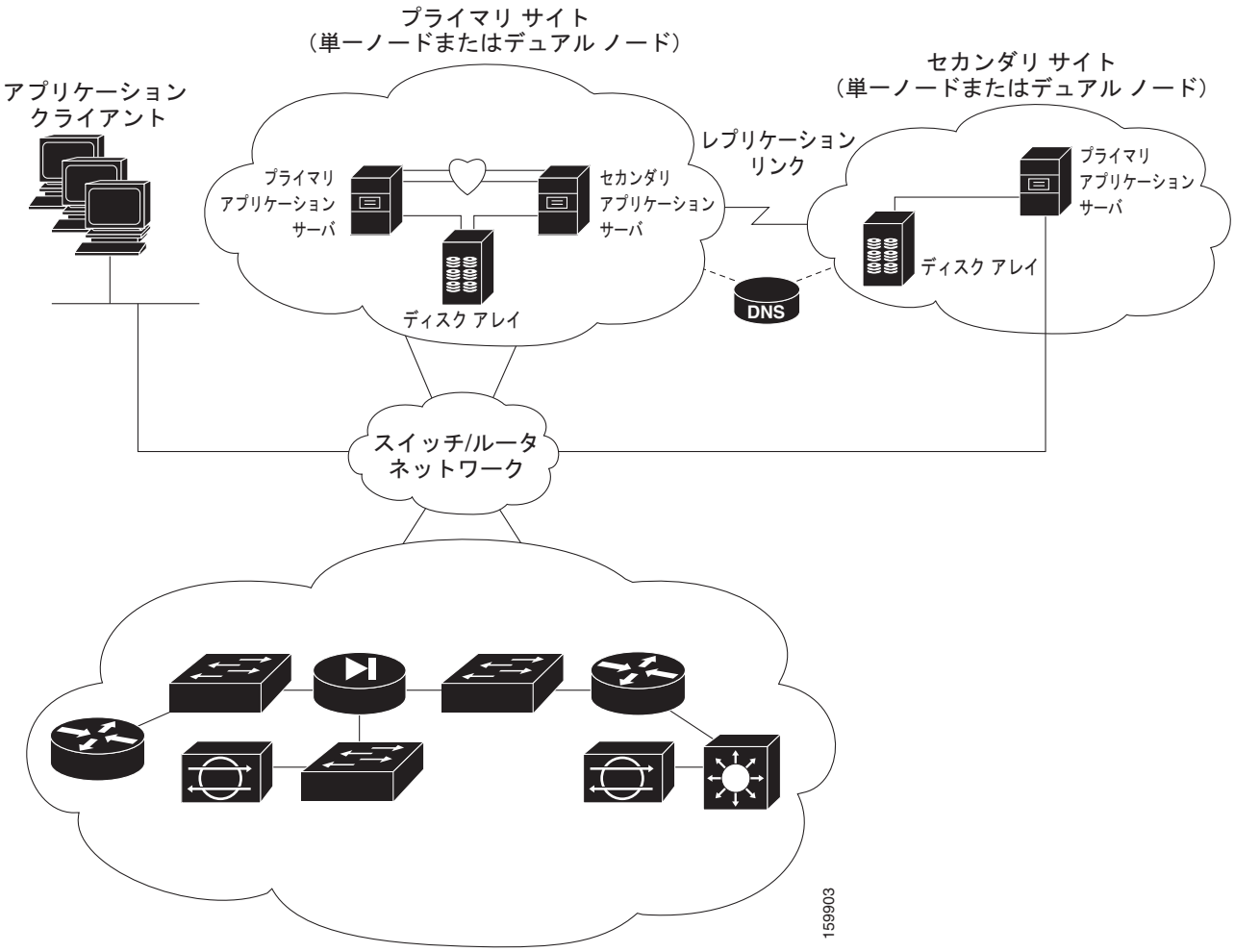
地理的冗長性（DR）プロセスの概要

地理的冗長性の構成では、2 つのサイト間でアプリケーション データを複製することにより、ディザスタ リカバリを提供します。サイト間のフェールオーバーを手動で開始するか、自動的に実行できます。

図 1-2 に、地理的冗長性（DR）の構成を示します。

（注）　図 1-2 のサーバには、ミラーリングされた内蔵ブート ディスクが含まれることがあります。同じメーカー、モデル、およびストレージ容量にすることを推奨します。サーバとの通信にはフォールトトレラントなスイッチド/ルーテッド ネットワークを推奨します。

図 1-2　地理的冗長性（DR）の構成



地理的冗長性（DR）の設定手順

次の表に、Cisco Security Manager の地理的な冗長性を持つインストールを設定するために必要な手順を示します。

	タスク	参照
ステップ 1	物理接続を確立します。	「イーサネット接続の確立」（P.3-1）
ステップ 2	Microsoft Windows サーバとすべての必要なドライバをインストールします。	「Microsoft Windows Server のインストール」（P.3-2）
ステップ 3	ストレージ接続を確立します。	「外部ストレージへのサーバの接続」（P.3-2）
ステップ 4	Symantec Veritas 製品およびコンポーネントをインストールして設定します。	「Symantec Veritas 製品のインストール」（P.3-2）

	タスク	参照
ステップ 5	ブート ディスクをミラーリングします。	「ブート ディスクのミラーリング（任意）」（P.3-3）
ステップ 6	共有アレイに必要なボリュームをセットアップします。	「Veritas Volume Manager の設定タスク」（P.3-4）
ステップ 7	プライマリ サーバの共有ボリューム上に Cisco Security Manager をインストールします。	「Security Manager のインストール」（P.3-6）
ステップ 8	セカンダリ サーバのスペア（ダミー）ボリューム上に Cisco Security Manager をインストールします。	「Security Manager のインストール」（P.3-6）
ステップ 9	複製を設定します。	「Veritas Volume Replicator タスク」（P.3-12）
ステップ 10	セカンダリ サーバに対する権限を更新します。	「作業ボリュームに対する権限の更新」（P.3-14）
ステップ 11	クラスタを作成し、設定します。	「Veritas Cluster Server タスク」（P.3-16）

Symantec Veritas 製品

このマニュアルで説明されている Security Manager HA/DR ソリューションは、Symantec VERITAS 製品に基づいています。ここでは、各 Veritas アプリケーションの概要を示します。

- Veritas Storage Foundation for Windows（VSFW）

  VSFW は、Windows 企業コンピューティング環境で、ボリューム管理テクノロジー、迅速なリカバリ、およびフォールト トレラント機能を提供します。VSFW は VCS および VVR の基盤を提供します。

- Veritas Cluster Server（VCS）

  VCS は、アプリケーションのダウン タイムを減らすためのクラスタリング ソリューションです。VCS の Global Cluster Option（GCO）は、（DR 構成などで使用される）複数のクラスタの管理をサポートします。

- Veritas Volume Replicator（VVR）

  VVR は、IP ネットワークを介して継続的にデータを複製することにより、リモート リカバリ サイトで重要なアプリケーションを迅速に、高い信頼性でリカバリできます。

- Veritas Enterprise Administrator（VEA GUI）コンソール

  VEA GUI コンソール ウィンドウは、システムのすべてのストレージ オブジェクトを表示および処理するためのグラフィカルな方法を提供します。

- Cluster Manager（Java コンソール）

  Cluster Manager（Java コンソール）は、クラスタのすべての管理機能を提供します。クラスタと、サービス グループ、システム、リソース、リソース タイプなどの VCS オブジェクトをモニタするには、Java コンソールのさまざまなビューを使用します。

  - Cluster Monitor

    Cluster Monitor は、実際のクラスタまたはシミュレートされたクラスタに関する一般情報を表示します。Cluster Monitor を使用して、クラスタへのログインやクラスタからのログオフ、さまざまな VCS オブジェクトのサマリー情報の表示、表示のカスタマイズ、VCS シミュレータの使用、および Cluster Manager の終了を行います。

- Cluster Explorer

  Cluster Explorer はクラスタ管理のメイン ウィンドウです。このウィンドウから、VCS オブジェクトのステータスを表示したり、さまざまな操作を実行したりできます。

CHAPTER 2

システム要件

この章では、HA または DR 環境に Security Manager をインストールするための参照構成について説明します。この章は、次の内容で構成されています。

- 「シングル ノード サイトのハードウェア要件」（P.2-1）
- 「デュアル ノード サイトのハードウェア要件」（P.2-2）
- 「ローカル冗長性構成のソフトウェア要件」（P.2-3）
- 「地理的冗長性（DR）構成のソフトウェア要件」（P.2-4）
- 「クラスタリングが不要な複製のソフトウェア要件」（P.2-4）
- 「プリインストール ワークシート」（P.2-5）

（注） 異なるハードウェア セットアップを使用する多くの構成があります。Microsoft と Symantec/Veritas のそれぞれのハードウェア互換性リスト（HCL）を参照してください。

（注） 当社は、Security Manager 用に指定されたサードパーティのハードウェアおよびソフトウェアのプラットフォームの可用性を確保するために最大限の努力をしますが、当社の制御を超えるサードパーティ ベンダー製品の可用性や変更によるシステム要件の変更または修正の権利を留保します。

シングル ノード サイトのハードウェア要件

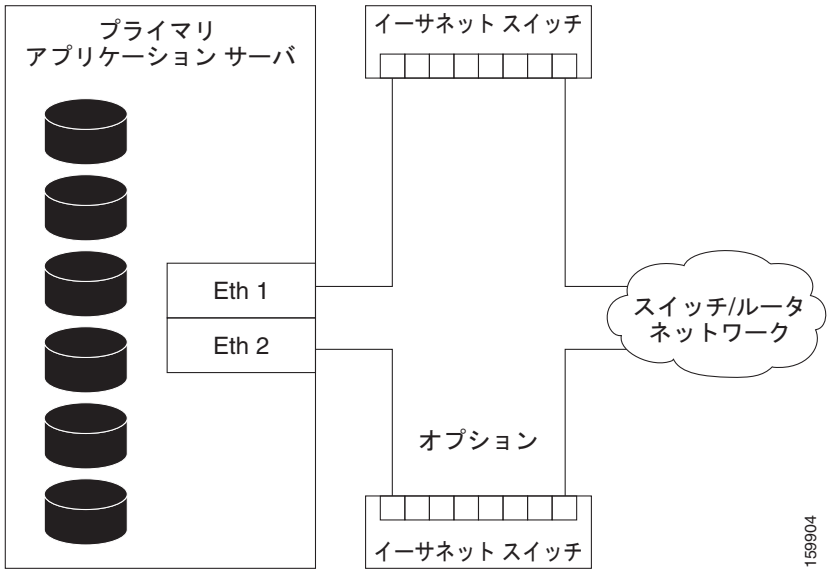
シングル ノードの HA 環境に Security Manager をインストールするには、フォールトトレラントなストレージ アレイを設定するか、内蔵ディスクを使用できます。

次は、シングル ノード サイトのサーバ ハードウェア仕様です。

- 『*Installation Guide for Cisco Security Manager 4.4*』に記載されているプロセッサと RAM の基本要件を満たすサーバ
- 1 つ以上のイーサネット インターフェイス（2 つを推奨）
- 2 台以上の物理ドライブ（6 台を推奨）

図 2-1 では、冗長性のためにサーバからスイッチ/ルータ ネットワークへの 2 本のイーサネット接続を使用しています。イーサネット ポートまたはスイッチで障害が発生しても、サーバとの通信は保持されます。このレベルのネットワーク冗長性が必要ない場合は、スイッチ/ルータ ネットワークへの 1 本の接続を使用できます（つまり、Eth 2 および関連するイーサネット スイッチは任意です）。

図 2-1　シングル ノード サイトのイーサネット接続



デュアル ノード サイトのハードウェア要件

デュアル ノード HA 環境に Security Manager をインストールするには、共有ストレージ アレイにアクセス可能な 2 台のサーバが必要です。

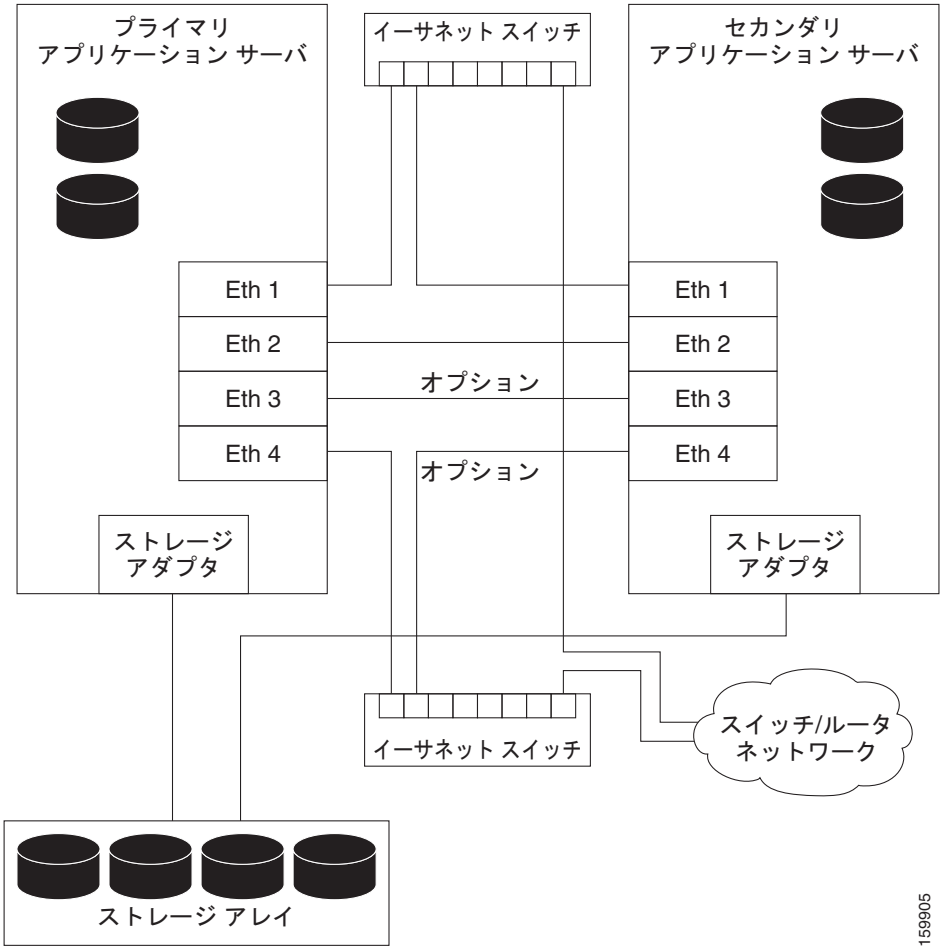
次は、デュアル ノード サイトのサーバ ハードウェア仕様です。

- 『*Installation Guide for Cisco Security Manager 4.4*』に記載されているプロセッサと RAM の基本要件を満たすサーバ
- 2 つ以上のイーサネット インターフェイス（4 つを推奨）
- 1 台以上の内蔵物理ドライブ（2 台を推奨）
- 1 台以上の外部ドライブ（2 台を推奨、複製を使用する場合は 4 台を推奨）

図 2-2 に、イーサネット接続および外部ストレージ接続を示すデュアル ノード サイトの構成を示します。冗長性のためにサーバからスイッチ/ルータ ネットワークへの 2 本のイーサネット接続が使用されています。イーサネット ポートまたはスイッチで障害が発生しても、サーバとの通信は保持されます。このレベルのネットワーク冗長性が必要ない場合は、スイッチ/ルータ ネットワークへの 1 本の接続を

使用できます（つまり、Eth 4 および関連するイーサネット スイッチは任意です）。クラスタのハートビート通信のためにサーバ間に 2 本の直接イーサネット接続が確立されていますが、2 本目のハートビート接続（Eth 3）は任意です。

図 2-2　　デュアル ノード サイトのイーサネット接続とストレージ接続



ローカル冗長性構成のソフトウェア要件

ローカル冗長性 HA 構成に Security Manager をインストールするには、次のソフトウェアが必要です。

- Cisco Security Management Suite 4.4
- Symantec Veritas Storage Foundation HA for Windows versions 5.1 SP1/6.0
- Symantec Dynamic Multipathing Option

Security Manager のライセンスは、HA/DR 構成のアクティブ サーバでのみ必要です。スタンバイ サーバの追加ライセンスは必要ではありません。

Veritas Storage Foundation HA for Windows は、ノードごとにライセンスされます。同じローカル冗長性構成の例では、各サーバに Veritas Storage Foundation HA for Windows を実行するためのライセンスが必要です。

Veritas Dynamic Multipathing Option は、サーバとストレージ間の複数のパスを提供する複数のホスト バス アダプタを搭載した外部ストレージをサーバで使用する場合にのみ必要です。

地理的冗長性（DR）構成のソフトウェア要件

地理的冗長性（DR）構成に Security Manager をインストールするには、次のソフトウェアが必要です。

- Cisco Security Management Suite 4.4
- Symantec Veritas Storage Foundation HA/DR for Windows 5.1 SP1/6.0
- Symantec Veritas Volume Replicator Option
- Symantec Veritas Dynamic Multipathing Option

Security Manager は、HA/DR 構成のアクティブ サーバごとにライセンスされます。たとえば、サイト A にシングル ノード クラスタ、サイト B にシングル ノード クラスタが配置された地理的冗長性構成では、Security Manager のコピーを 1 つのみ購入する必要があります。これは、Security Manager は常に 1 台のサーバでのみアクティブになるためです。

Veritas Storage Foundation HA for Windows は、ノードごとにライセンスされます。2 台のサーバ（クラスタごとに 1 台）が配置された同じ地理的冗長性構成の例では、各サーバに Veritas Storage Foundation HA for Windows を実行するためのライセンスが必要です。

Veritas Volume Replicator Option は、ノードごとにライセンスされます。

Veritas Dynamic Multipathing Option は、サーバとストレージ間の複数のパスを提供する複数のホスト バス アダプタを搭載した外部ストレージをサーバで使用する場合にのみ必要です。

クラスタリングが不要な複製のソフトウェア要件

クラスタリングが不要な地理的冗長性（DR）構成に Security Manager をインストールするには、次のソフトウェアが必要です。

- Cisco Security Management Suite 4.4
- Symantec Veritas Storage Foundation Basic for Windows 5.1 SP1/6.0
- Symantec Veritas Volume Replicator Option
- Symantec Veritas Dynamic Multipathing Option

Security Manager は、HA/DR 構成のアクティブ サーバごとにライセンスされます。たとえば、プライマリ サーバとセカンダリ サーバの間で複製が実行される地理的冗長性構成では、Security Manager のコピーを 1 つのみ購入する必要があります、これは、Security Manager は常に 1 台のサーバでのみアクティブになるためです。

Veritas Storage Foundation for Windows は、ノードごとにライセンスされます。2 台のサーバが配置された同じ地理的冗長性構成の例では、各サーバに Veritas Storage Foundation for Windows を実行するためのライセンスが必要です。

Veritas Storage Foundation Basic for Windows Version 5.1 SP1/6.0 は、最大 4 つのボリュームと連携し、Symantec から無料でダウンロードできます。

Veritas Volume Replicator Option は、ノードごとにライセンスされます。

Veritas Dynamic Multipathing Option は、サーバとストレージ間の複数のパスを提供する複数のホスト バス アダプタを搭載した外部ストレージをサーバで使用する場合にのみ必要です。

プリインストール ワークシート

インストールを計画して設定中に必要な情報を収集するには、プリインストール ワークシートを使用します。ここでは、次の項目について説明します。

- 「ローカル冗長性構成のワークシート」（P.2-5）
- 「地理的冗長性（DR）設定ワークシート」（P.2-6）

ローカル冗長性構成のワークシート

ローカル冗長性 HA 構成に Security Manager をインストールする前に、表 2-1 に記載されたインストールの完了に役立つ情報を書き留めます。

表 2-1　ローカル冗長性構成のプリインストール ワークシート

情報	プライマリ サイト	
共有ディスク グループ名	**datadg**	
共有ボリューム名	**cscopx**	
Security Manager データのドライブ文字		
イベント データの共有ディスク グループ名[1]	**datadg_evt**	
イベント データの共有ボリューム名[1]	**cscopx_evt**	
Security Manager イベント データのドライブ文字[1]		
クラスタ名	**CSManager_Primary**	
クラスタ ID	0[2]	
Security Manager 仮想 IP アドレス/サブネット マスク		
クラスタ サービスの仮想 IP アドレス/サブネット マスク[3]		
	プライマリ サーバ	**セカンダリ サーバ**
ホスト名		
パブリック ネットワーク インターフェイス #1 と IP アドレス/サブネット マスク		
パブリック ネットワーク インターフェイス #2[4] と IP アドレス/サブネット マスク		
プライベート クラスタ相互接続 #1		
プライベート クラスタ相互接続 #2		

1. 任意：別に保存されたイベント データが必要な場合は、これらのフィールドを使用します。
2. 0 ～ 255 の整数で、同一サブネット上のクラスタで一意にする必要があります。
3. これは、Security Manager 仮想 IP アドレス/サブネット マスクと同じ値です。
4. 冗長性を確保するためにパブリック ネットワークへのアクセスに 2 番目の NIC を使用する場合に必要です。

地理的冗長性（DR）設定ワークシート

地理的冗長性（DR）構成に Security Manager をインストールする場合は、表 2-2 に記載されたインストールの完了に役立つ情報を書き留めます。

表 2-2　地理的冗長性（DR）構成のプリインストール ワークシート

情報	プライマリ サイト		セカンダリ サイト	
ディスク グループ	**datadg**		**datadg**	
データ ボリューム	**cscopx**		**cscopx**	
Security Manager のドライブ文字				
イベント データのディスク グループ[1]	**datadg_evt**		**datadg_evt**	
イベント データのデータ ボリューム	**cscopx_evt**		**cscopx_evt**	
イベント データのドライブ文字				
Storage Replicator Log ボリューム	**data_srl**		**data_srl**	
複製されたデータ セット	**CSM_RDS**			
複製されたボリューム グループ	**CSM_RVG**			
クラスタ名	**CSManager_Primary**		**CSManager_Secondary**	
クラスタ ID	**0**[2]		**1**[2]	
Security Manager 仮想 IP アドレス/サブネット マスク				
複製仮想 IP アドレス/サブネット マスク				
クラスタ サービスの仮想 IP アドレス/サブネット マスク[3,4]				
	プライマリ サーバ	**セカンダリ サーバ**	**プライマリ サーバ**	**セカンダリ サーバ**
ホスト名				
パブリック ネットワーク インターフェイス #1 と IP アドレス/サブネット マスク				
パブリック ネットワーク インターフェイス #2 と IP アドレス/サブネット マスク[5]				
プライベート クラスタ相互接続 #1[6]				
プライベート クラスタ相互接続 #2[6]				

1. 任意：別に保存されたイベント データが必要な場合は、これらのフィールドを使用します。
2. 0 ～ 255 の整数で、同一サブネット上のクラスタで一意にする必要があります。
3. 2 台のサーバまたは複数のアダプタを使用してパブリック ネットワークにアクセスするクラスタでのみ必要です。1 つのネットワーク アダプタのみを使用してパブリック ネットワークにアクセスする単一サーバ クラスタでは、このアダプタの固定 IP アドレスを使用できます。
4. これは、Security Manager 仮想 IP アドレス/サブネット マスクと同じ値です。

5. 冗長性を確保するためにパブリック ネットワークへのアクセスに 2 番目の NIC を使用する場合に必要です。
6. 2 台のサーバを使用するクラスタでのみ必要です。

CHAPTER 3

Cisco Security Management Suite ハイ アベイラビリティ ソリューションのインストール

この章では、HA または DR の展開構成に Security Manager をインストールする方法について説明します。次のタスクをリストされた順番に実行する必要がありますが、一部のタスクは任意であるか、または構成に応じて適用されない可能性があります。

この章は、次の内容で構成されています。

- 「イーサネット接続の確立」（P.3-1）
- 「Microsoft Windows Server のインストール」（P.3-2）
- 「外部ストレージへのサーバの接続」（P.3-2）
- 「Symantec Veritas 製品のインストール」（P.3-2）
- 「ブート ディスクのミラーリング（任意）」（P.3-3）
- 「Veritas Volume Manager の設定タスク」（P.3-4）
- 「Security Manager のインストール」（P.3-6）
- 「Veritas Volume Replicator タスク」（P.3-12）
- 「作業ボリュームに対する権限の更新」（P.3-14）
- 「Veritas Cluster Server タスク」（P.3-16）

イーサネット接続の確立

HA または DR 構成で必要なイーサネット接続を確立するには、次の手順に従います。

ステップ 1 クラスタ構成に応じて、図 2-1 または図 2-2 のようにサーバとスイッチ間のイーサネット接続を確立します。

（注） サーバごとのルータ / スイッチ ネットワークへの 2 本目のイーサネット接続の使用は任意ですが、NIC またはローカル イーサネット スイッチで障害が発生した場合に、冗長性のレベルが高くなります。Veritas Cluster Server（VCS）には、IPMultiNicPlus エージェントが含まれます。このエージェントを使用すると、サーバ上に複数の NIC カードをセットアップできるため、サーバにルータ / スイッチ ネットワークへの冗長アクセスが提供されます。NIC カードの障害、ケーブルの取り外し、その他の障害が発生すると、VCS は障害を検出し、サーバ上の別

の動作している NIC カードに動作する仮想 IP アドレスを再割り当てできます。IPMultiNicPlus エージェントの詳細については、『Veritas Cluster Server Bundled Agents Reference Guide』を参照してください。このマニュアルの例では、ネットワーク アクセスのために単一の NIC カードを使用するケースを示します。

代わりに、ベンダー固有の NIC チーミング（IEEE 802.3ad リンク集約）ソリューションを使用することもできます。

ステップ 2　デュアル ノード クラスタの場合は、図 2-2 に従って、サーバ間にイーサネット クラスタ通信接続を確立します。サーバ間を直接接続する場合は、インターフェイスが自動クロスオーバー検出をサポートするかどうかによって、クロスオーバー イーサネット ケーブルを使用する必要がないことがあります。ほとんどの新しいイーサネット インターフェイスではこの機能がサポートされ、別のサーバに直接接続するときにストレート ケーブルを使用できます。

Microsoft Windows Server のインストール

サポートされている Microsoft Windows オペレーティング システムをインストールします。

Microsoft Windows Server 2008 R2 Service Pack 1（64 ビット）Enterprise Edition

Microsoft Windows Server 2008 Service Pack 2（64 ビット）Enterprise Edition

すべてのサーバで同じオペレーティング システムを使用することを推奨します。

（注）　Symantec Veritas Storage Foundation HA for Windows version 5.1 SP1/6.0 を使用するには、すべてのシステムで同じパスにオペレーティング システムをインストールする必要があります。たとえば、あるノードの C:\WINDOWS に Windows をインストールする場合、他のすべてのノードで C:\WINDOWS にインストールする必要があります。同じドライブ文字がすべてのノードで使用可能であり、システム ドライブにインストール用の十分な領域があることを確認します。

外部ストレージへのサーバの接続

デュアル ノード クラスタを使用する場合は、共有外部ストレージが必要です。『*Hardware Compatibility List for Veritas Storage Foundation & High Availability Solutions for Windows*』のストレージ ハードウェアを使用できます。シングル ノード クラスタでは内部ストレージまたは外部ストレージのどちらかを使用できます。

Symantec Veritas 製品のインストール

Symantec Veritas 製品およびコンポーネントをインストールして設定します。シングル ローカル クラスタ、デュアル地理的クラスタ、またはクラスタリングが不要な複製を使用するがどうかに応じて、必要な製品およびコンポーネントが異なります。Volume Manager の GUI（Veritas Enterprise Administrator）など、一部のコンポーネントは任意です。表 3-1 を参照してください。

表 3-1　Veritas ソフトウェア コンポーネント

Veritas 製品 / コンポーネント	シングル ローカル クラスタ	デュアル地理的クラスタ	クラスタリングが不要な複製
Storage Foundation for Windows	—	—	必要
Symantec Veritas Storage Foundation HA for Windows version 5.1 SP1/6.0	必要	必要	—
Volume Replicator Option	不要	必要	必要
Global Cluster Option	不要	必要	—
Dynamic Multipathing Option	「注」を参照[1]	「注」を参照[1]	「注」を参照[1]
Veritas Enterprise Administrator（GUI）[2]	必要	必要	必要
Cluster Manager（GUI）[2]	オプション	オプション	—

1. サーバとディスク ストレージ間の複数のパスを提供する複数のホスト バス アダプタを搭載した外部ストレージを使用する場合にのみ必要です。
2. サーバまたは別のクライアント マシンにインストールできます。

Veritas ソフトウェアのインストールの前提条件および手順については、Veritas の該当するリリース ノートおよびインストール ガイドを参照してください。

（注）　1 つの重要な前提条件は、Windows Server ドメインの一部としてサーバを設定することです。

ブート ディスクのミラーリング（任意）

ブート ディスクのミラーリングは任意です。ただし、これにより、特定のサーバの保護が強化されます。ブート ディスクで障害が発生すると、ミラーリングされた代替ブート ディスクから起動することにより、マシンを迅速にリカバリできます。ミラーリングは、ブート ディスクを Veritas Volume Manager の制御下のダイナミック ディスク グループに配置し、ミラーを追加することによって実現されます。

この手順の詳細については『Symantec Veritas Storage Foundation HA for Windows version 5.1 SP1/6.0 administrator's guide』の「Set up a Dynamic Boot and System Volume」の項を参照してください。

Veritas Volume Manager の設定タスク

ここでは、Security Manager アプリケーションで必要なディスク グループおよびボリュームを設定します。設定は、サーバがプライマリ サーバまたはセカンダリ サーバであるかどうか、および複製が関係するかどうかによって異なります。VEA GUI またはコマンドラインから Volume Manager タスクを実行できます。VEA またはコマンドラインを使用したこれらの手順の詳細については、『Symantec Veritas Storage Foundation HA for Windows version 5.1 SP1/6.0 administrator's guide』を参照してください。

ここでは、次の項目について説明します。

- 「プライマリ サーバ（複製なし）」（P.3-4）
- 「プライマリ サーバ（複製あり）」（P.3-5）
- 「セカンダリ サーバとセカンダリ クラスタ内のプライマリ サーバ」（P.3-6）

プライマリ サーバ（複製なし）

複製が関係しないシングル クラスタ構成でプライマリ サーバ上の Security Manager に必要なディスク グループおよびボリュームを設定するには、次の手順を使用します。シングル クラスタ構成では、クラスタ内のすべてのサーバにアクセス可能な外部共有ストレージが使用されます。

ディスク グループおよびボリュームを設定するには、次の手順に従います。

ステップ 1　次の特性を持つディスク グループを作成します。

- グループ名：**datadg**
- タイプ：**ダイナミック（クラスタ）**
- ディスク数：ソフトウェア RAID を使用する場合、ミラーリング対象としてグループに少なくとも 2 台のディスクを含めます。それ以外の場合は、1 台の論理ディスク（ハードウェア RAID を使用）で十分です。このディスク グループに使用するディスクは、クラスタ内のすべてのノードにアクセス可能である必要があります。

（注）　ソフトウェア RAID 5 の使用は推奨されません。

ステップ 2　次の特性を持つボリュームを **datadg** ディスク グループに作成します。

- ボリューム名：**cscopx**
- 割り当てられたドライブ文字：**<Selected Drive Letter>**

（注）　使用可能なドライブ文字を選択できます。ただし、ドライブ文字は、すべてのシステムで同じである必要があります。

- ファイル タイプ：**NTFS**

プライマリ サーバ（複製あり）

2 つのクラスタ間で複製が実行されるデュアル地理的構成でプライマリ サーバ上の Security Manager に必要なディスク グループおよびボリュームを設定するには、次の手順を使用します。プライマリ クラスタとセカンダリ クラスタの両方のプライマリ サーバでこの手順を実行します。各クラスタについて、シングル ノード クラスタまたは共有ストレージを使用する複数ノード クラスタを使用できます。ただし、このマニュアルでは、デュアル地理的構成の複数ノード クラスタのケースについては説明しません。

ディスク グループおよびボリュームを設定するには、次の手順に従います。

ステップ 1　次の特性を持つディスク グループを作成します。

- グループ名：**datadg**
- タイプ：**ダイナミック（クラスタ）**（VCS を使用する場合）、**ダイナミック（セカンダリ）**（VCS を使用しない場合）
- ディスク数 : ソフトウェア RAID を使用する場合、ミラーリング対象としてグループに少なくとも 2 台のディスクを含めます。それ以外の場合は、1 台の論理ディスク（ハードウェア RAID を使用）で十分です。これが複数ノード クラスタの場合、このディスク グループに使用するディスクは、クラスタ内のすべてのノードにアクセス可能である必要があります。

（注）　ソフトウェア RAID 5 の使用は推奨されません。

ステップ 2　次の特性を持つボリュームを **datadg** ディスク グループに作成します。

- ボリューム名：**cscopx**
- 割り当てられたドライブ文字：**<Selected Drive Letter>**（プライマリ クラスタの場合）、**なし**（セカンダリ クラスタの場合）
- ファイル タイプ：**NTFS**（プライマリ クラスタの場合）、なし（セカンダリ クラスタの場合）
- ボリュームのロギング：**なし**

ステップ 3　**datadg** ディスク グループに、Storage Replicator Log（SRL）として使用する次の特性を持つボリュームを作成します。

- ボリューム名：**data_srl**
- 割り当てられたドライブ文字：**なし**
- ファイル タイプ：**Unformatted**
- ボリュームのロギング：**なし**

（注）　SRL の適正なサイズの選択の詳細については、『Volume Replicator administrator's guide』を参照してください。

セカンダリ サーバとセカンダリ クラスタ内のプライマリ サーバ

セカンダリ サーバおよびセカンダリ クラスタ内のプライマリ サーバに Security Manager をインストールするために必要なディスク グループおよびボリュームを設定するには、次の手順を使用します。すべてのセカンダリ サーバおよびセカンダリ クラスタ内のプライマリ サーバに Security Manager をインストールする必要があります。このような場合、スペア ボリュームに Security Manager をインストールします。スペア ボリュームは、インストール前に一時的にマウントされてからマウント解除され、Security Manager をサーバからアンインストールするか、またはアップグレードするまで再利用されません。プライマリ クラスタのプライマリ サーバに使用されたものと同じドライブ文字に一時ボリュームをマウントし、インストール時に同じインストール パス（たとえば、F:\Program Files\CSCOpx）を使用する必要があります。

ディスク グループおよびボリュームを設定するには、次の手順に従います。

ステップ 1　既存のディスク グループにスペア ボリュームを作成していない場合は、次の特性を持つディスク グループを作成します。

- グループ名：**datadg_spare**
- タイプ：**ダイナミック（セカンダリ）**
- サイズ：**5 GB**（ボリュームには、Security Manager をインストールするのに十分な容量のみ必要）
- ディスク数：このディスク グループはアプリケーション データの格納に使用されないため、1 台の非冗長ディスクで十分です。

ステップ 2　次の特性を持つボリュームをディスク グループに作成します。

- ボリューム名：**cscopx_spare**
- 割り当てられたドライブ文字：**<Selected Drive Letter>**

（注）　プライマリ サーバの cscopx ドライブに使用したのと同じドライブ文字を使用する**必要があります**。

- ファイル タイプ：**NTFS**

Security Manager のインストール

Security Manager のインストーラは、Symantec Veritas Storage Foundation HA for Windows version 5.1 SP1/6.0 の存在を検出し、HA/DR 構成に Security Manager をインストールするかどうかを確認します。このオプションを選択した場合、通常のインストール時に加えて指定する唯一の情報はデータベース パスワードです。非 HA/DR インストールでは、データベース パスワードが自動的に生成されます。ただし、データベース パスワードは HA/DR 構成のすべてのサーバで同じにする必要があるため、インストーラはパスワードを指定するよう要求します。HA/DR 構成のすべてのサーバでこの同じパスワードを使用する必要があります。

HA/DR インストールによって VCS 用 Cisco Security Manager エージェントがインストールされるため、VCS は新しい **CSManager** リソース タイプを認識し、Security Manager を制御およびモニタできます。

また、Veritas Cluster Server が代わりに HA/DR 構成の各サーバにおける Security Manager の起動と停止を制御するため、Windows の Security Manager とその関連サービスのスタートアップの種類が自動ではなく手動として設定されます。そうしないと、Security Manager が常に 1 台のサーバでのみ実行される場合、Security Manager アプリケーションは、サーバのリブート後に HA/DR 構成のすべてのサーバで開始しようとします。

HA/DR 構成の各サーバに Security Manager をインストールする必要があります。ただし、HA/DR 構成では、Security Manager のプライマリ インスタンスだけが使用され、保護されます。その他のインストールは、構成内のセカンダリ サーバのいずれかでプライマリ インスタンスを実行できるようにするために実行されます。

ここでは、次の項目について説明します。

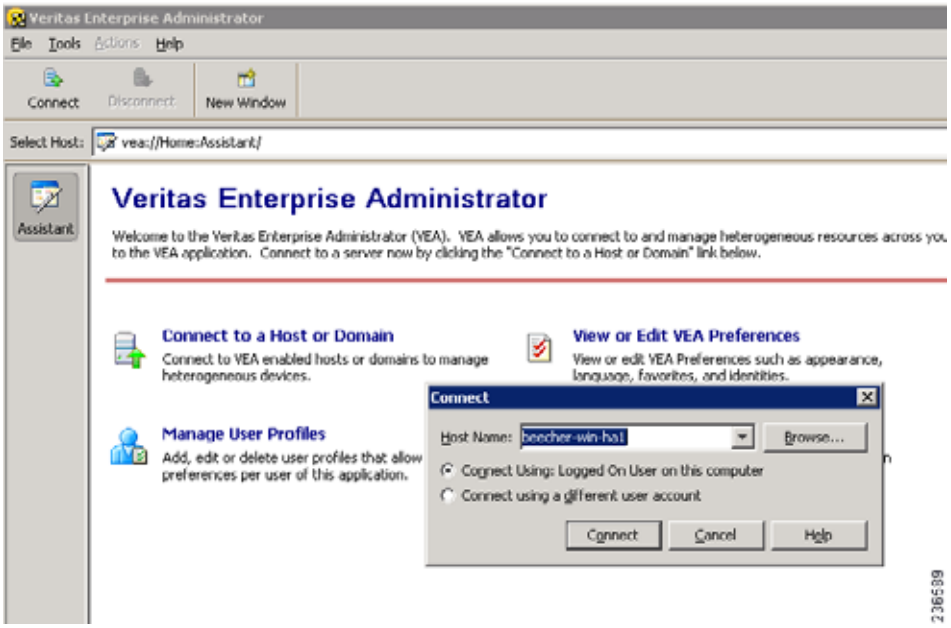
- 「プライマリ サーバへの Security Manager のインストール」（P.3-7）
- 「セカンダリ サーバへの Security Manager のインストール」（P.3-9）

プライマリ サーバへの Security Manager のインストール

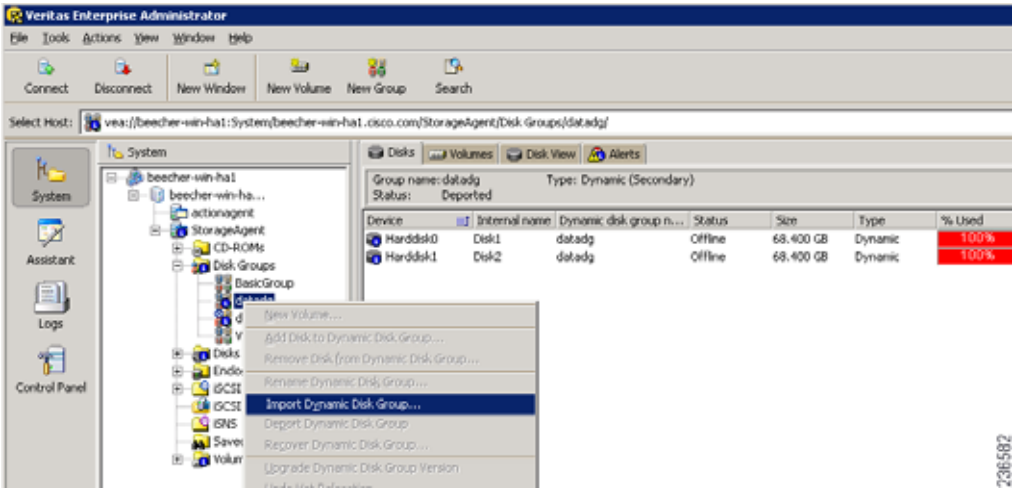
実稼働環境で使用され、HA/DR 構成によって保護される Security Manager のプライマリ インスタンスをインストールするには、次の手順を使用します。

プライマリ サーバ上に Security Manager をインストールするには、次の手順に従います。

ステップ 1　クラスタ内のプライマリ サーバで、Veritas Enterprise Administrator（VEA GUI）アプリケーションを開き、ログインします。



ステップ 2　**datadg** ディスク グループを右クリックし、[Import Dynamic Disk Group] を選択します。



ステップ 3　[Import as dynamic disk group] オプションが選択されていることを確認し、[OK] をクリックします。

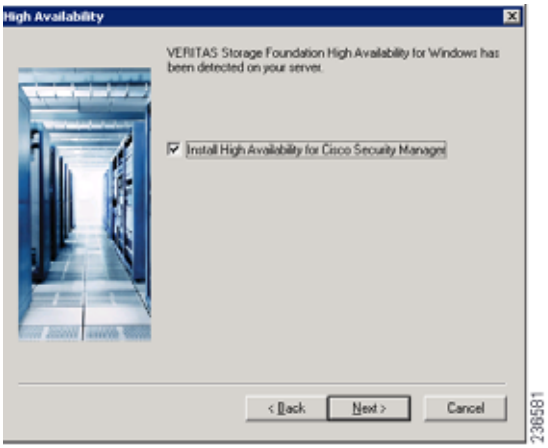
ステップ 4　[System] の [Volumes] フォルダを展開します。

ステップ 5　**cscopx** ボリュームを右クリックし、[File System] > [Change Drive Letter and Path] を選択します。

ステップ 6　目的のドライブ文字を **cscopx** ボリュームに割り当て、[OK] をクリックします。ドライブの割り当てについては、「ローカル冗長性構成のワークシート」（P.2-5）または「地理的冗長性（DR）設定ワークシート」（P.2-6）を参照してください。

ステップ 7　次の HA 固有の項目に注意しながら『Security Manager Installation Guide』に従って Security Manager をインストールします。

a. HA 用に Security Manager をインストールするかどうかを尋ねるプロンプトが表示されたら、ボックスをオンにして yes を指定します。



b. インストール ディレクトリの入力を求められたら、[*<Selected Drive Letter>:\Program Files\CSCOpx*] を指定します。

c. データベース パスワードの指定を求められたら、適切なパスワードを選択し、忘れないようにします。HA/DR 構成のすべての Security Manager サーバにこのパスワードを使用します。

（注）　Security Manager のインストールの終了に近づくと、マルチホーム サーバを使用することと、gatekeeper.cfg ファイルを更新する必要があることを示すメッセージが表示されることがあります。HA/DR 構成で使用されるエージェントのスクリプトがこのファイルを修正するため、このメッセージは無視できます。

ステップ 8　Security Manager のインストール後、サーバをリブートします。

ステップ 9　システムのリブート後、VEA GUI を開き、共有ディスク グループがインポートされているかどうかを確認します。ディスク グループのステータスがオフラインの場合、ステップ 2 ～ステップ 6 を繰り返してディスク グループをインポートし、インストール時に使用されたのと同じドライブ文字を割り当てます。

ステップ 10　online.pl スクリプトを使用して Security Manager を起動します。詳細については、「Security Manager の手動での起動、停止、またはフェールオーバー」（P.4-3）を参照してください。

（注）　Security Manager の正常動作に必要な Windows レジストリ エントリの設定を完了するために、Security Manager を起動する必要があります。

ステップ 11　Security Manager の起動が完了するまで 5 ～ 10 分間待機してから、URL として **http://<server hostname or IP address>:1741** を使用してアプリケーションの Web インターフェイスにログインします。正常にログインできることを確認します。

ヒント　または、**pdshow** コマンドを使用して、Cisco Security Manager サービスが正常に動作していることを確認することもできます。

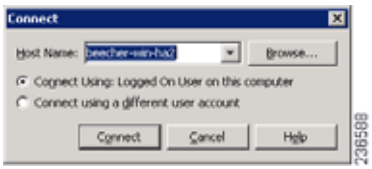
ステップ 12　アプリケーションの Web インターフェイスからログアウトし、offline.pl スクリプトを使用して Security Manager を停止します。詳細については、「Security Manager の手動での起動、停止、またはフェールオーバー」（P.4-3）を参照してください。

セカンダリ サーバへの Security Manager のインストール

セカンダリ サーバに Security Manager をインストールするには、次の手順を使用します。セカンダリ サーバへの Security Manager のインストールは、プライマリ サーバへのインストールに似ていますが、重要な違いが 1 つあります。Security Manager をスペア ボリューム（**cscopx_spare**）にインストールします。スペア ボリュームは、特定のセカンダリ サーバに関連付けられ、Security Manager をアップグレードまたはアンインストールする場合に限り、再利用されます。このスペア ボリュームには、空のデータベース（～ 2 GB）で Security Manager アプリケーションを保持するのに十分な容量が必要です。十分な領域が（可能であれば別のディスク グループで）使用可能な場合は、**datadg** ディスク グループにスペア ボリュームを作成できます。

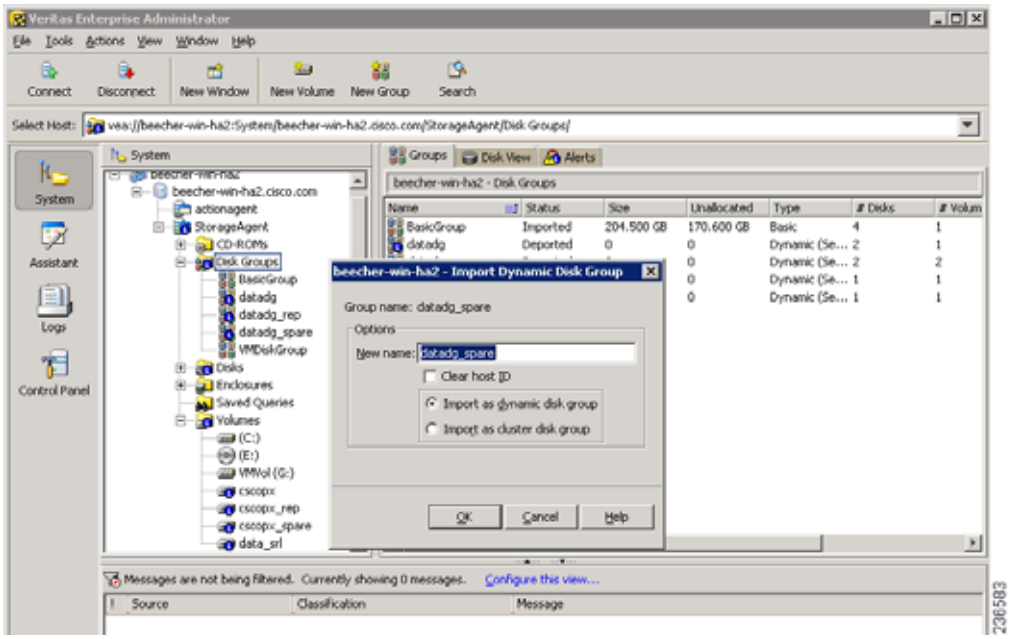
セカンダリ サーバ上に Security Manager をインストールするには、次の手順に従います。

ステップ 1　セカンダリ サーバで、Veritas Enterprise Administrator（VEA GUI）アプリケーションを開き、ログインします。



ステップ 2　**datadg_spare** ディスク グループを右クリックし、[Import Dynamic Disk Group] を選択します。

ステップ 3　[Import as dynamic disk group] オプションが選択されていることを確認し、[OK] をクリックします。



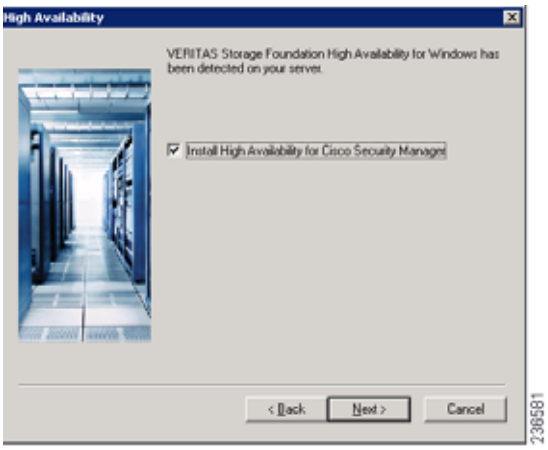
ステップ 4　[System] の [Volumes] フォルダを展開します。

ステップ 5　**cscopx_spare** ボリュームを右クリックし、[File System] > [Change Drive Letter and Path] を選択します。

ステップ 6　目的のドライブ文字を **cscopx_spare** ボリュームに割り当て、[OK] をクリックします。ドライブの割り当てについては、「ローカル冗長性構成のワークシート」（P.2-5）または「地理的冗長性（DR）設定ワークシート」（P.2-6）を参照してください。

ステップ 7　次の HA 固有の項目に注意しながら『Security Manager Installation Guide』に従って Security Manager をインストールします。

a.　HA 用に Security Manager をインストールするかどうかを尋ねるプロンプトが表示されたら、ボックスをオンにして yes を指定します。



b. インストール ディレクトリの入力を求められたら、[*<Selected Drive Letter>:\Program Files\CSCOpx*] を指定します。

c. データベース パスワードの指定を求められたら、プライマリ サーバに選択したのと同じパスワードを選択します。

（注） Security Manager のインストールの終了に近づくと、マルチホーム サーバを使用することと、gatekeeper.cfg ファイルを更新する必要があることを示すメッセージが表示されることがあります。HA/DR 構成で使用されるオンライン スクリプトがこのファイルを修正するため、このメッセージは無視できます。

ステップ 8　Security Manager のインストール後、サーバをリブートします。

ステップ 9　システムのリブート後、VEA GUI を開き、共有ディスク グループがインポートされているかどうかを確認します。ディスク グループのステータスがオフラインの場合、ステップ 2 ～ステップ 6 を繰り返してディスク グループをインポートし、インストール時に使用されたのと同じドライブ文字を割り当てます。

ステップ 10　online.pl スクリプトを使用して Security Manager を起動します。詳細については、「Security Manager の手動での起動、停止、またはフェールオーバー」（P.4-3）を参照してください。

（注） Security Manager の正常動作に必要な Windows レジストリ エントリの設定を完了するために、Security Manager を起動する必要があります。

ステップ 11　Security Manager の起動が完了するまで 5 ～ 10 分間待機してから、URL として **http://<server hostname or IP address>:1741** を使用してアプリケーションの Web インターフェイスにログインします 正常にログインできることを確認します。

ヒント　または、**pdshow** コマンドを使用して、Cisco Security Manager サービスが正常に動作していることを確認することもできます。

ステップ 12　アプリケーションの Web インターフェイスからログアウトし、offline.pl スクリプトを使用して Security Manager を停止します。詳細については、「Security Manager の手動での起動、停止、またはフェールオーバー」（P.4-3）を参照してください。

ステップ 13　インストールの完了後、スペア ボリュームのドライブ文字の割り当てを解除します。

Veritas Volume Replicator タスク

クラスタ間で複製が動作するデュアル地理的クラスタ構成の複製を設定するには、次の手順を使用します。

複製を設定するには、次の手順に従います。

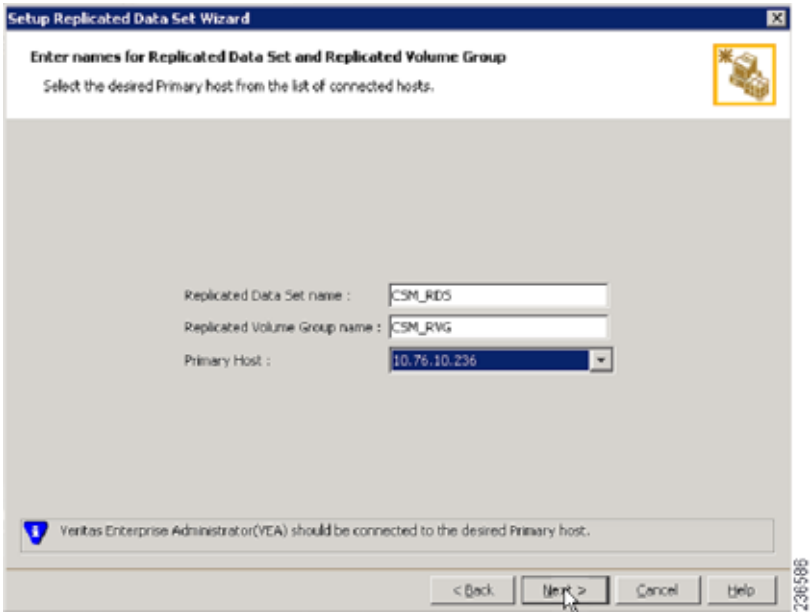
ステップ 1　VEA GUI を使用して、プライマリおよびセカンダリ ホストに接続します。

ステップ 2　*datadg* ディスク グループがプライマリ サーバとセカンダリ サーバの両方にインポートされていることを確認します。

ステップ 3　[View] > [Connection] > [Replication Network] を選択します。

ステップ 4　ツリーから [Replication Network] を選択し、ツールバーから [Setup Replicated Data Set] ウィザードを選択します。ウィザードの最初のパネルで次の項目を指定します。

- [Replicated Data Set Name] : **CSM_RDS**
- [Replicated Volume Group name] : **CSM_RVG**
- ドロップダウン リストからプライマリ ホストを選択します。



ステップ 5　[Next] をクリックし、[Select Dynamic Disk Group and volumes to be replicated] パネルで次の項目を指定します。

- [Dynamic Disk Group] : **datadg**
- Volumes : **cscopx**

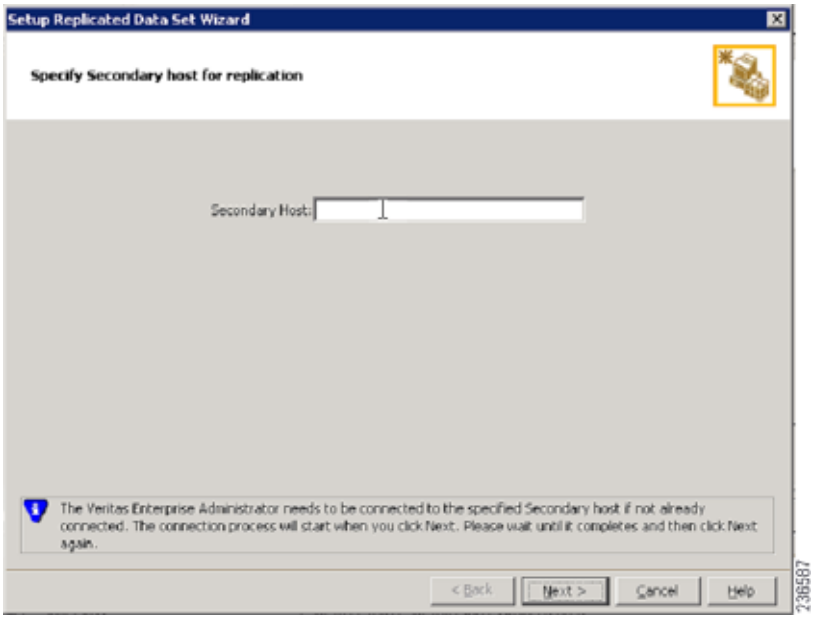
ステップ 6　[Next] をクリックします。data_srl が他に利用できる唯一のボリュームの場合、レプリケータ ログのストレージ ボリュームとして自動的に認識されます。複数の追加ボリュームを使用できる場合、[Storage Replicator Log] パネルが表示されます。次のことを指定します。

- [Volume for the Replicator Log] : **data_srl**

ステップ 7　[Next] をクリックし、サマリー情報を確認してから、[Create Primary RVG] をクリックして RVG を作成します。

ステップ 8　正常にプライマリ RVG を作成した後、RDS へのセカンダリ ホストの追加を求められたら、[Yes] をクリックします。

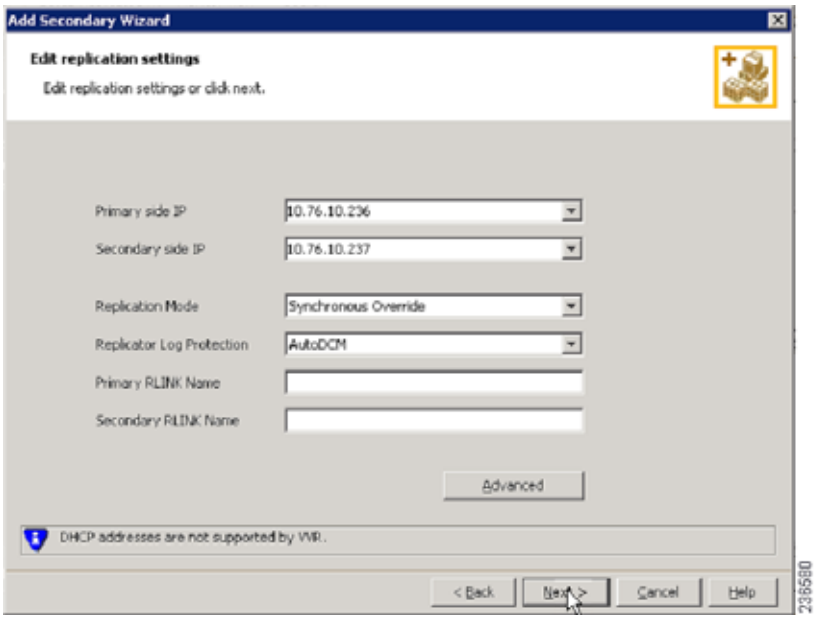
ステップ 9　[Specify Secondary host for replication] パネルで、[Secondary Host] フィールドにセカンダリ ホストの名前または IP アドレスを入力します。



ステップ 10　[Next] をクリックし、[Edit replication settings] パネルで次の項目を指定します。

（注）　プライマリおよびセカンダリ側の IP アドレスについては、NIC カードの固定 IP アドレスを指定できます。ただし、Veritas Cluster Server を使用する場合は、後で戻って VCS の制御下の仮想 IP アドレスを使用するように IP アドレスを更新する必要があります。VEA のツリーでセカンダリ RVG を選択し、[Actions] > [Change Replication Settings] を選択して、これを実行します。

- [Primary side IP] : <IP address of the primary server>
- [Secondary side IP] : <IP address of the secondary server>
- [Replication Mode] : [Synchronous Override]
- [Replicator Log Protection]:<Choose from **Off**, **Fail**, **DCM**, **AutoDCM** (Default), **Override**>。各選択肢の説明については、『Volume Replicator administrator's guide』を参照してください。



ステップ 11　[Next] をクリックして、デフォルトの設定で複製を開始します。[Synchronize Automatically] を選択し、[Start Replication] がオンになっていることを確認します。

ステップ 12　[Next] をクリックして [Summary] ページを表示してから [Finish] をクリックします。

作業ボリュームに対する権限の更新

Security Manager をインストールすると、Security Manager を実行するための特別なローカル ユーザ（casuser）とグループ（casusers）が作成されます。セカンダリ サーバで Security Manager の保護されたインスタンスを実行するには、cscopx ボリュームにローカル casusers グループ権限を追加する必要があります。

ここでは、次の項目について説明します。

- 「共有ストレージを使用する場合の権限の更新」（P.3-14）
- 「複製を使用する場合の権限の更新」（P.3-15）

共有ストレージを使用する場合の権限の更新

共有ストレージを使用する場合にセカンダリ サーバに対するローカル casusers グループ権限を追加するには、次の手順に従います。

ステップ 1　プライマリ サーバで実行されている場合は、offline.pl スクリプトを使用して Security Manager を停止します。詳細については、「Security Manager の手動での起動、停止、またはフェールオーバー」（P.4-3）を参照してください。

ステップ 2　プライマリ サーバから **datadg** ディスク グループをデポートします。

ステップ 3　セカンダリ サーバに **datadg** ディスク グループをインポートします。

ステップ 4　VEA GUI またはコマンドラインを使用して、選択したドライブ文字にプライマリ ボリューム（cscopx）を割り当てます。

ステップ 5　Windows Explorer で、**<Selected Drive Letter>:\Program Files\CSCOpx** フォルダを右クリックし、[Sharing and Security] メニュー項目を選択します。

ステップ 6　フォルダ プロパティのダイアログボックスが表示されます。[Security] タブを選択して [Add] をクリックします。

ステップ 7　[Select Users or Groups] ダイアログボックスの [Location] をクリックし、選択ツリーからローカル サーバを選択します。

ステップ 8　オブジェクト名を入力するテキストボックスに **casusers** を入力し、[Check Names] をクリックします。テキスト ボックスに、*<ServerName>\casusers* が表示されます。[OK] をクリックします。

ステップ 9　casuser が選択されていることを確認し、[Allow] の下の [Full Control] チェックボックスをオンにして、casusers グループに完全な制御権限を付与します。

ステップ 10　[Advanced] をクリックします。

ステップ 11　[Advanced Settings] で、[Replace permission entries on all child objects with entries shown here that apply to child objects] チェックボックスをオンにします。

ステップ 12　[Apply] をクリックし、CSCOpx ディレクトリのすべての子オブジェクトに権限が伝播されるまで待機します。

ステップ 13　伝播が完了したら、[OK] をクリックします。

ステップ 14　[OK] をクリックして [CSCOpx Properties] ダイアログボックスを閉じます。

ステップ 15　cscopx ボリュームのドライブ文字の割り当てを解除します。

ステップ 16　セカンダリ サーバから datadg ディスク グループをデポートします。

ステップ 17　プライマリ サーバに datadg ディスク グループをインポートします。

ステップ 18　VEA GUI またはコマンドラインを使用して、選択したドライブ文字にプライマリ ボリューム（cscopx）を割り当てます。

複製を使用する場合の権限の更新

複製を使用する場合にセカンダリ サーバに対するローカル casusers グループ権限を追加するには、次の手順に従います。

ステップ 1　プライマリ サーバで実行されている場合は、offline.pl スクリプトを使用して Security Manager を停止します。詳細については、「Security Manager の手動での起動、停止、またはフェールオーバー」（P.4-3）を参照してください。

ステップ 2　cscopx ボリュームのドライブ文字の割り当てを解除します。

ステップ 3　複製のプライマリをセカンダリに移行します。

ステップ 4　セカンダリ サーバの cscopx ボリュームに選択したドライブ文字を割り当てます。

ステップ 5　Windows Explorer で、**<Selected Drive Letter>:\Program Files\CSCOpx** フォルダを右クリックし、[Sharing and Security] メニュー項目を選択します。

ステップ 6　フォルダ プロパティのダイアログボックスが表示されます。[Security] タブを選択して [Add] をクリックします。

ステップ 7　[Select Users or Groups] ダイアログボックスの [Location] をクリックし、選択ツリーからローカル サーバを選択します。

ステップ 8　オブジェクト名を入力するテキストボックスに **casusers** を入力し、[Check Names] をクリックします。テキスト ボックスに、<*ServerName*>*casusers* が表示されます。[OK] をクリックします。

ステップ 9　casuser が選択されていることを確認し、[Allow] の下の [Full Control] チェックボックスをオンにして、casusers グループに完全な制御権限を付与します。

ステップ 10　[Advanced] をクリックします。

ステップ 11　[Advanced Settings] で、[Replace permission entries on all child objects with entries shown here that apply to child objects] チェックボックスをオンにします。

ステップ 12　[Apply] をクリックし、CSCOpx ディレクトリのすべての子オブジェクトに権限が伝播されるまで待機します。

ステップ 13　伝播が完了したら、[OK] をクリックします。

（注）　権限の更新中に、「Error Applying Security」というタイトルのエラー ダイアログに「An error occurred applying security information to: <*Selected Drive Letter*>:\Program Files\CSCOpx\log\dcr.log Access is denied.」というメッセージが表示されることがあります。このエラーを無視し、エラー ダイアログで [Continue] をクリックして権限の更新プロセスを完了できます。

ステップ 14　[OK] をクリックして [CSCOpx Properties] ダイアログボックスを閉じます。

ステップ 15　cscopx ボリュームのドライブ文字の割り当てを解除します。

ステップ 16　プライマリ サーバに複製を戻します。

ステップ 17　プライマリ サーバの cscopx ボリュームに選択したドライブ文字を割り当てます。

Veritas Cluster Server タスク

ここでは、Veritas クラスタのセットアップおよび設定のプロセスについて説明します。2 つの特定のシナリオについて説明します。

「シングル ローカル クラスタ（デュアル ノード）構成」（P.3-16）

「デュアル地理的クラスタ構成」（P.3-25）

シングル ローカル クラスタ（デュアル ノード）構成

ここでは、クラスタ内に 2 ノード（プライマリとセカンダリ）を持つシングル ローカル クラスタのセットアップおよび設定について説明します。

ここでは、次の項目について説明します。

- 「クラスタの作成」（P.3-17）
- 「アプリケーション サービス グループの作成」（P.3-17）
- 「ClusterService グループの作成（任意）」（P.3-24）

クラスタの作成

クラスタを作成するには、次の手順に従います。

ステップ 1　VCS クラスタ設定ウィザードを使用してクラスタを作成します。

- Cluster Name = CSManager_Primary
- Cluster ID = 0

クラスタの定義にプライマリ サーバとセカンダリ サーバを含めます。ウィザードのクラスタ定義の一部はプライベート ネットワークの NIC を指定します。VCS は、クラスタ メンテナンスでのクラスタ ノード間の通信のためにプライベート ネットワークを使用します。すべての専用クラスタ通信インターフェイスに障害が発生した場合に、プライオリティが低いクラスタ通信インターフェイスとして動作するように、ネットワーク イーサネット インターフェイスの 1 を割り当てることもできます。

ステップ 2　Cluster Manager を起動するには、[Start] > [All Programs] > [Symantec] > [Veritas Cluster Server] > [Veritas Cluster Manager - Java Console] を選択し、クラスタにログインします。

ステップ 3　Cluster Manager を使用し、[File] > [Import Types] を選択して、CSManager リソース タイプをインポートします。$VCS_ROOT\cluster server\conf\config の下にある CSManagerTypes.cf ファイルを参照し、[Import] をクリックします。

アプリケーション サービス グループの作成

アプリケーション サービス グループを作成するには、次の手順に従います。

ステップ 1　CSManager リソースを右クリックし、[Add Service Group] を選択します。

APP というサービス グループを追加し、このサービス グループの両方のサーバを含めて（各サーバの [Startup] オプションをオンにする）、サービス グループ タイプを [Failover] にします。

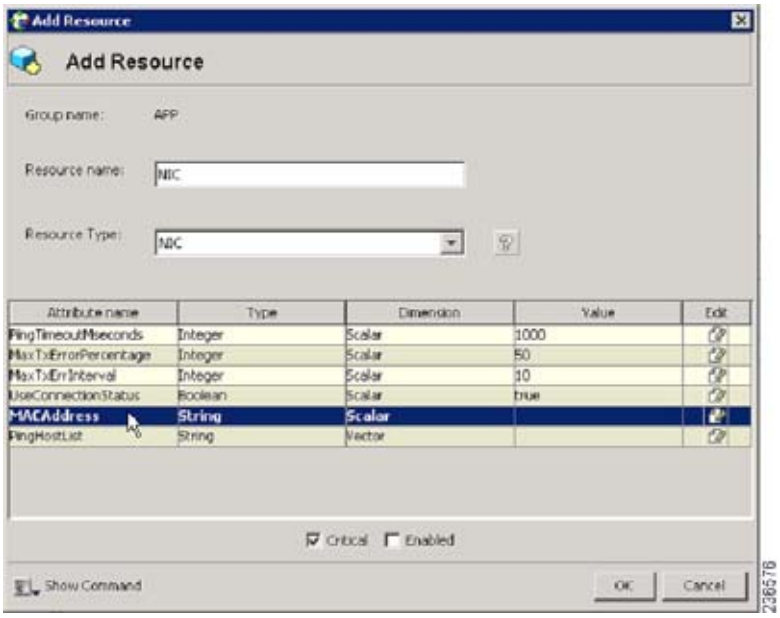
ステップ 2　[APP] サービス グループを右クリックし、[Add Resource] を選択します。

NIC リソースを追加し、[Critical] および [Enabled] チェックボックスをオンにします。

- Resource name = **NIC**
- Resource Type = **NIC**

- MACAddress = <MAC address of the NIC used for accessing the Security Manager application>
（クラスタ内のサーバごとに一意に定義されます）。

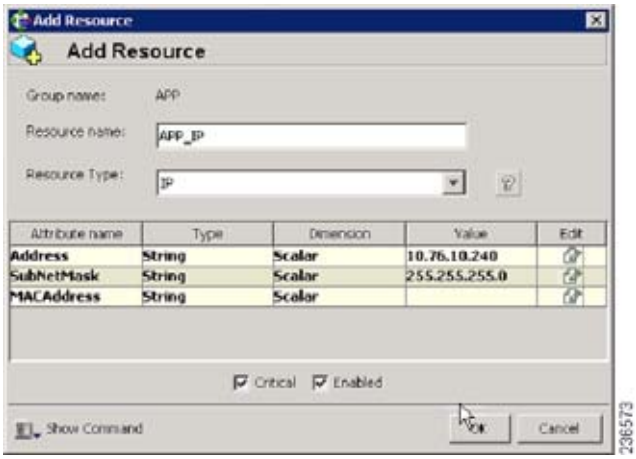
（注）　DOS レベルのコマンド **ipconfig -all** を使用して、各イーサネット インターフェイスに関連付けられた MAC アドレスを検索できます。



ステップ 3　[APP] サービス グループを右クリックし、[Add Resource] を選択します。

IP リソースを追加し、[Critical] および [Enabled] チェックボックスをオンにします。

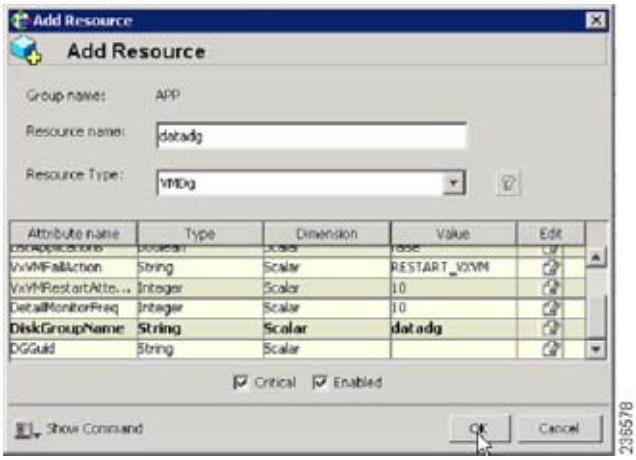
- Resource name = **APP_IP**
- Resource Type = **IP**
- Address = <Virtual IP address allocated for use by the Security Manager application>
（グローバル属性として定義されます）
- SubNetMask = <subnet mask>
（グローバル属性として定義されます）
- MACAddress = <MAC Address of the NIC used for accessing the Security Manager application>
（クラスタ内のサーバごとに定義されます）



ステップ 4　[APP] サービス グループを右クリックし、[Add Resource] を選択します。

VMDg リソースを追加し、[Critical] および [Enabled] チェックボックスをオンにします。

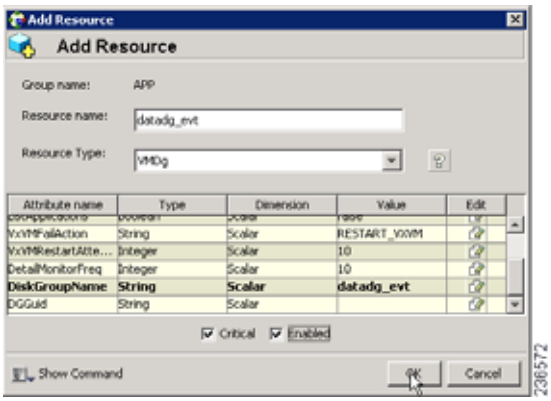
- Resource name = **datadg**
- Resource Type = **VMDg**
- DiskGroupName = **datadg**
  （グローバル属性として定義されます）



ステップ 5　[VMDg] リソース グループを右クリックし、[Add Resource] を選択します。

datadg_evt リソースを追加し、[Critical] および [Enabled] チェックボックスをオンにします。

- Resource name = **datadg_evt**
- Resource Type = **VMDg**
- DiskGroupName = **datadg_evt**
  （グローバル属性として定義されます）



ステップ 6　[APP] サービス グループを右クリックし、[Add Resource] を選択します。

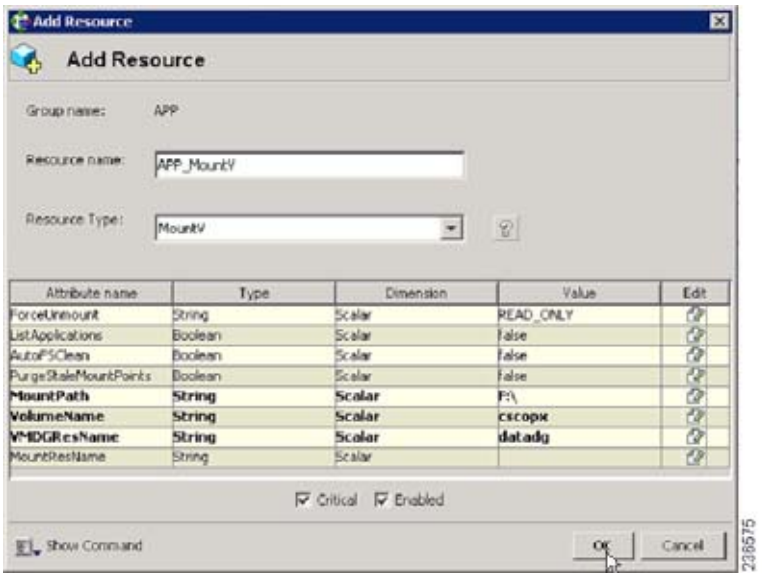
MountV リソースを追加し、[Critical] および [Enabled] チェックボックスをオンにします。

- Resource name = **APP_MountV**
- Resource Type = **MountV**
- MountPath = <Selected Drive Letter>:\
  （グローバル属性として定義されます）
- VolumeName = **cscopx**
  （グローバル属性として定義されます）
- VMDGResName = **datadg**
  （グローバル属性として定義されます）
- ForceUnmount = {NONE, READ-ONLY, ALL}

  他のアプリケーションで使用されている場合に、エージェントが強制的にボリュームをアンマウントするかどうかを定義します。次のオプションを利用できます。

  - [NONE]：エージェントは、アプリケーションがアクセスしている場合は、ボリュームをアンマウントしません。
  - [READ-ONLY]：エージェントは、アプリケーションが読み取り専用モードでアクセスしている場合に、ボリュームをアンマウントします。
  - [ALL]：エージェントは、アプリケーションが持つアクセス権の種類に関係なくボリュームをアンマウントします。

  デフォルトは [NONE] です。ボリュームをアンマウントできない場合、セカンダリ サーバへの自動フェールオーバーが禁止されている場合があるため、[READ-ONLY] または [ALL] の値の選択が必要になることがあります。



ステップ 7　[MountV] リソース グループを右クリックし、[Add Resource] を選択します。

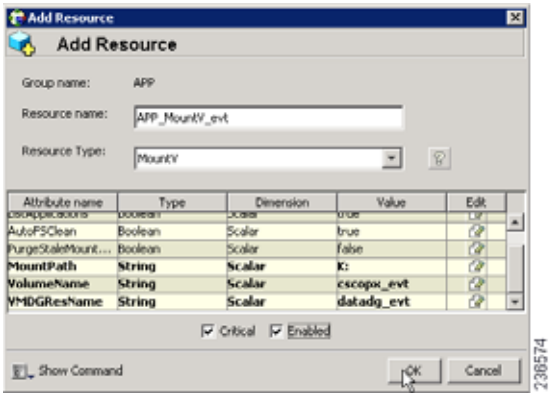
MountV_evt リソースを追加し、[Critical] および [Enabled] チェックボックスをオンにします。

- Resource name = **APP_MountV_evt**
- Resource Type = **MountV**
- MountPath = <Selected Drive Letter>:\
  （グローバル属性として定義されます）
- VolumeName = **cscopx_evt**
  （グローバル属性として定義されます）
- VMDGResName = **datadg_evt**
  （グローバル属性として定義されます）
- ForceUnmount = {NONE, READ-ONLY, ALL}

  他のアプリケーションで使用されている場合に、エージェントが強制的にボリュームをアンマウントするかどうかを定義します。次のオプションを利用できます。

  - [NONE]：エージェントは、アプリケーションがアクセスしている場合は、ボリュームをアンマウントしません。
  - [READ-ONLY]：エージェントは、アプリケーションが読み取り専用モードでアクセスしている場合に、ボリュームをアンマウントします。
  - [ALL]：エージェントは、アプリケーションが持つアクセス権の種類に関係なくボリュームをアンマウントします。

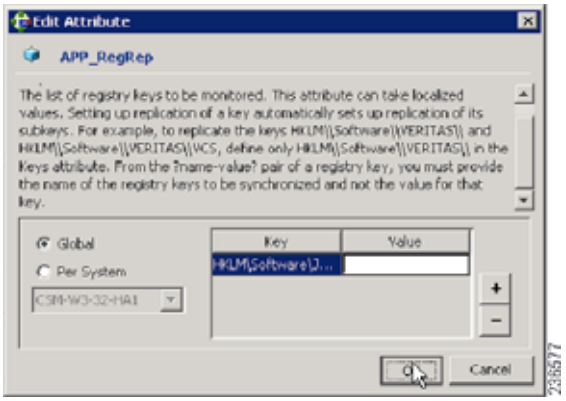
  デフォルトは [NONE] です。ボリュームをアンマウントできない場合、セカンダリ サーバへの自動フェールオーバーが禁止されている場合があるため、[READ-ONLY] または [ALL] の値の選択が必要になることがあります。



ステップ 8　[APP] サービス グループを右クリックし、[Add Resource] を選択します。

RegRep リソースを追加し、[Critical] および [Enabled] チェックボックスをオンにします。

- Resource name = **APP_RegRep**
- Resource Type = **RegRep**
- MountResName = **APP_MountV**
  （グローバル属性として定義されます）
- ReplicationDirectory = **\REGREP\DEFAULT**
  （グローバル属性として定義されます）
- キー（グローバル属性として定義されます）
  Key = **HKLM\Software\JavaSoft\Prefs\vms**
  Value = <blank>



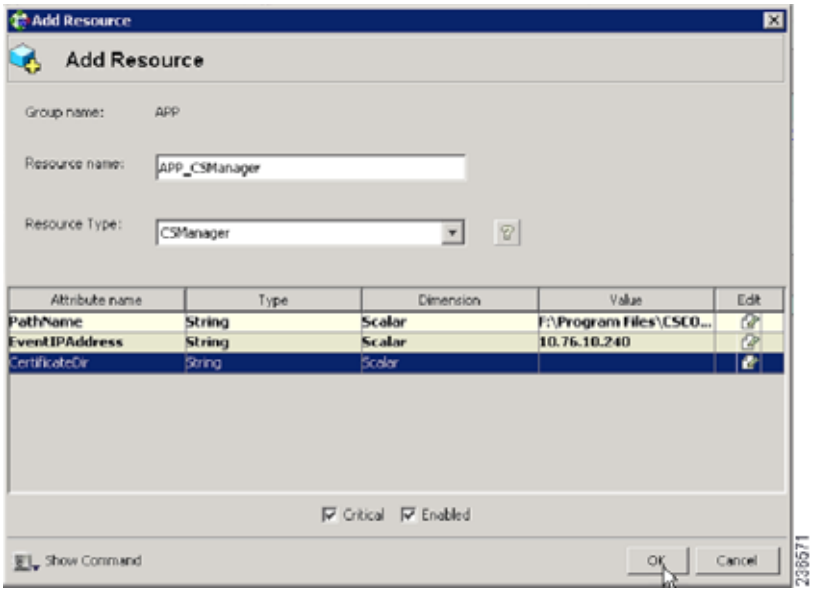
（注）　Security Manager は、サーバ レジストリの HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Prefs\vms の下にクライアント ユーザ プリファレンスを保存します。レジストリ複製エージェント（RegRep）は、アクティブ サーバの指定レジストリの場所の変更をモニタし、フェールオーバーの発生時にセカンダリ サーバにこれらの変更を同期化します。

ステップ 9　[APP] サービス グループを右クリックし、[Add Resource] を選択します。

CSManager リソースを追加し、[Critical] および [Enabled] チェックボックスをオンにします。

- Resource name = **APP_CSManager**

- Resource Type = **CSManager**
- PathName = **<Selected Drive Letter>:\Program Files\CSCOpx**
  （グローバル属性として定義されます）
- EventIPAddress = APP_IP で使用されているものと同じ IP アドレス
  （グローバル属性として定義されます）
- CertificateDir = この属性の説明については、「SSL 用のセキュリティ証明書」（P.4-2）を参照してください。



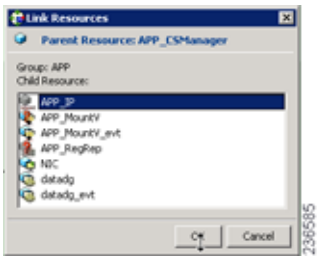
ステップ 10　次の表の定義に従ってリソースをリンクします（図 A-1（P.A-2）を参照）。

親リソース	子リソース
APP_CSManager	APP_RegRep
APP_CSManager	APP_IP
APP_IP	NIC
APP_RegRep	APP_MountV
APP_RegRep	APP_MountV_evt
APP_MountV	datadg
APP_MountV_evt	datadg_evt

リソースをリンクするには、次の手順に従います。

a. 親リソースを右クリックし、[Link] を選択します。

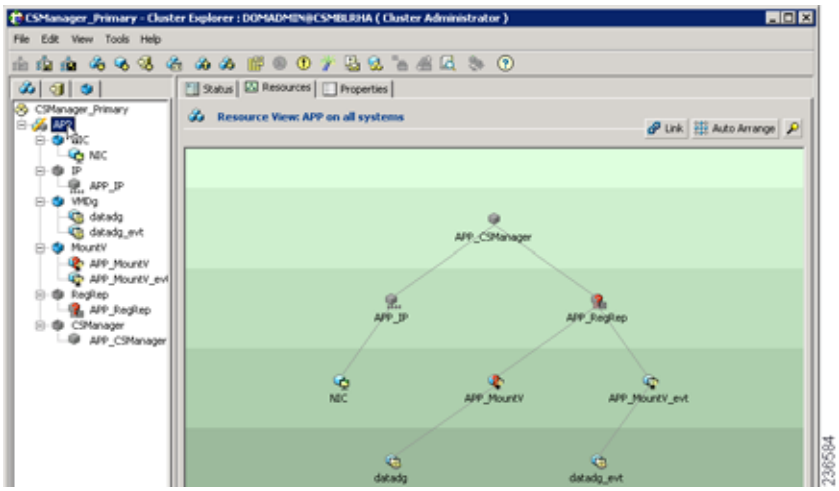
[Link Resources] ダイアログボックスが表示されます。



b. 子リソースを選択し、[OK] をクリックします。

選択したリソースがリンクされます。

すべてのリンクが作成されると、リソース ビューは次のように表示されます。



ClusterService グループの作成（任意）

次のオプション コンポーネントを実行して、ClusterService グループを設定することもできます。

- Cluster Manager（Web コンソール）
- 通知

これらのコンポーネントの設定に VCS 設定ウィザードを使用できます。詳細については、『Veritas Cluster Server administrator's guide』を参照してください。通知サービスは、クラスタで発生するイベントを電子メールまたは SNMP トラップを介して通知できるため便利です。

デュアル地理的クラスタ構成

ここでは、各クラスタ内に 1 つのノードを含む、地理的に離れた 2 つのクラスタのセットアップと設定について説明します。

（注）　一方または両方のクラスタ内に複数のノードがあるデュアル地理的クラスタ構成を作成することもできます。

ここでは、次の項目について説明します。

- 「プライマリおよびセカンダリ クラスタの作成」（P.3-25）
- 「ClusterService グループの作成」（P.3-26）
- 「複製サービス グループの作成」（P.3-27）
- 「アプリケーション サービス グループの作成」（P.3-28）
- 「クラスタ レベル設定の作成」（P.3-30）

プライマリおよびセカンダリ クラスタの作成

プライマリ クラスタとセカンダリ クラスタを作成するには、次の手順を実行します。

ステップ 1　VCS クラスタ設定ウィザードを使用して、（プライマリ クラスタ内の）プライマリ サーバでクラスタを作成します。

- Cluster Name = CSManager_Primary
- Cluster ID = 0

ステップ 2　VCS クラスタ設定ウィザードを使用して、（セカンダリ クラスタ内の）プライマリ サーバでクラスタを作成します。

- Cluster Name = CSManager_Secondary
- Cluster ID = 1

ステップ 3　プライマリ クラスタで、[Start] > [All Programs] > [Symantec] > [Veritas Cluster Server] > [Veritas Cluster Manager - Java Console] を選択して Cluster Manager を起動し、クラスタにログインします。

ステップ 4　Cluster Manager を使用し、[File] > [Import Types] を選択して、CSManager リソース タイプをインポートします。$VCS_ROOT\cluster server\conf\config の下にある CSManagerTypes.cf ファイルを参照し、[Import] をクリックします。

ステップ 5　セカンダリ クラスタに対してステップ 3 と 4 を繰り返します。

ClusterService グループの作成

ClusterService グループを作成するには、次の手順を実行します。

（注）　プライマリ クラスタとセカンダリ クラスタの両方で次の手順を実行します。

ヒント　クラスタ間の通信用に ClusterService グループおよび wac リソースを作成するためのこの項の手順に代わる方法として VCS 設定ウィザードを使用できます。VCS 設定ウィザードでオプションの Cluster Manager（Web コンソール）と通知コンポーネントを設定することもできます。『Veritas Cluster Server administrator's guide』を参照してください。

ステップ 1　CSManager リソースを右クリックし、[Add Service Group] を選択します。

ClusterService というサービス グループを追加します。

ステップ 2　[ClusterService] サービス グループを右クリックし、[Add Resource] を選択します。

NIC リソースを追加します。

- Resource name = **NIC**
- Resource Type = **NIC**
- MACAddress = <MAC Address of the NIC card>

（注）　DOS レベルのコマンド **ipconfig -all** を使用して、各イーサネット インターフェイスに関連付けられた MAC アドレスを検索できます。

ステップ 3　[ClusterService] サービス グループを右クリックし、[Add Resource] を選択します。

IP リソースを追加します

- Resource name = **VCS_IP**
- Resource Type = **IP**
- Address = <Virtual IP address allocated for the cluster>
- SubNetMask = <subnet mask>
- MACAddress = <MAC Address of the corresponding NIC card>

ステップ 4　[ClusterService] サービス グループを右クリックし、[Add Resource] を選択します。

wac リソースを追加します。

- Resource name = **wac**
- Resource Type = **Process**
- StartProgram = **C:\Program Files\Veritas\Cluster Server\bin\wac.exe**
- StopProgram = **C:\Program Files\Veritas\Cluster Server\bin\wacstop.exe**
- MonitorProgram = **C:\Program Files\Veritas\Cluster Server\bin\wacmonitor.exe**

ステップ 5　次の表の定義に従ってリソースをリンクします（図 A-4（P.A-4）を参照）。

親リソース	子リソース
wac	VCS_IP
VCS_IP	NIC

リソースをリンクするには、次の手順に従います。

a. 親リソースを右クリックし、[Link] を選択します。
[Link Resources] ダイアログボックスが表示されます。

b. 子リソースを選択し、[OK] をクリックします。
選択したリソースがリンクされます。

複製サービス グループの作成

複製サービス グループを作成するには、次の手順に従います。

（注）　プライマリ クラスタとセカンダリ クラスタの両方で次の手順を実行します。

ステップ 1　CSManager リソースを右クリックし、[Add Service Group] を選択します。
APPrep というサービス グループを追加します。

ステップ 2　[APPrep] サービス グループを右クリックし、[Add Resource] を選択します。
Proxy リソースを追加します。

- Resource name = **VVR_NIC_Proxy**
- Resource Type = **Proxy**
- TargetResName = **NIC**

ステップ 3　[APPrep] サービス グループを右クリックし、[Add Resource] を選択します。
IP リソースを追加します。

- Resource name = **VVR_IP**
- Resource Type = **IP**
- Address = <Virtual IP address allocated for replication>
- SubNetMask = <subnet mask>
- MACAddress = <MAC address of the corresponding NIC card>

ステップ 4　[APPrep] サービス グループを右クリックし、[Add Resource] を選択します。
VMDg リソースを追加します。

- Resource name = **datadg**
- Resource Type = **VMDg**
- DiskGroupName = **datadg**

ステップ 5　[APPrep] サービス グループを右クリックし、[Add Resource] を選択します。

VvrRvg リソースを追加します。

- Resource name = **APP_RVG**
- Resource Type = **VvrRvg**
- RVG = **CSM_RVG**
- VMDGResName = **datadg**
- IPResName = **VVR_IP**

ステップ 6　次の表の定義に従ってリソースをリンクします（図 A-3（P.A-3）を参照）。

親リソース	子リソース
VVR_IP	VVR_NIC_Proxy
APP_RVG	VVR_IP
APP_RVG	datadg

リソースをリンクするには、次の手順に従います。

a. 親リソースを右クリックし、[Link] を選択します。
[Link Resources] ダイアログボックスが表示されます。

b. 子リソースを選択し、[OK] をクリックします。
選択したリソースがリンクされます。

アプリケーション サービス グループの作成

アプリケーション サービス グループを作成するには、次の手順に従います。

（注）　プライマリ クラスタとセカンダリ クラスタの両方で次の手順を実行します。

ステップ 1　APP というサービス グループを追加します。

ステップ 2　[APP] サービス グループを右クリックし、[Add Resource] を選択します。
RVG プライマリ リソースを追加します。

- Resource name = **APP_RVGPrimary**
- Resource Type = **RVGPrimary**
- RvgResourceName = **APP_RVG**

ステップ 3　[APP] サービス グループを右クリックし、[Add Resource] を選択します。
MountV リソースを追加します。

- Resource name = **APP_MountV**
- Resource Type = **MountV**
- Mount Path = <Selected Drive Letter>:\
- Volume Name = **cscopx**
- VMDg Resource Name = **datadg**

ステップ 4　[APP] サービス グループを右クリックし、[Add Resource] を選択します。

RegRep リソースを追加し、[Critical] および [Enabled] チェックボックスをオンにします。

- Resource name = **APP_RegRep**
- MountResName = **APP_MountV**
- ReplicationDirectory = **\REGREP\DEFAULT**
- Keys = **HKLM\Software\JavaSoft\Prefs\vms**

（注） Security Manager は、サーバ レジストリの HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Prefs\vms の下にクライアント ユーザ プリファレンスを保存します。レジストリ複製エージェント（RegRep）は、アクティブ サーバの指定レジストリの場所の変更をモニタし、フェールオーバーの発生時にセカンダリ サーバにこれらの変更を同期化します。

ステップ 5　[APP] サービス グループを右クリックし、[Add Resource] を選択します。

Proxy リソースを追加します。

- Resource name = **APP_NIC_Proxy**
- Resource Type = **Proxy**
- TargetResName = **NIC**

ステップ 6　[APP] サービス グループを右クリックし、[Add Resource] を選択します。

IP リソースを追加します。

- Resource name = **APP_IP**
- Resource Type = **IP**
- Address = <Virtual IP address allocated for the application>
- SubNetMask = <subnet mask>
- MACAddress = <MAC address of the corresponding NIC card>

ステップ 7　[APP] サービス グループを右クリックし、[Add Resource] を選択します。

CSManager リソースを追加します。

- Resource name = **APP_CSManager**
- Resource Type = **CSManager**
- PathName = <***Selected Drive Letter***>**:\Program Files\CSCOpx**
- EventIPAddress = APP_IP で使用されているものと同じ IP アドレス
- CertificateDir = この属性の説明については、「SSL 用のセキュリティ証明書」（P.4-2）を参照してください。

ステップ 8　次の表の定義に従ってリソースをリンクします（図 A-2（P.A-3）を参照）。

親リソース	子リソース
APP_MountV	APP_RVGPrimary
APP_RegRep	APP_MountV
APP_CSManager	APP_RegRep

親リソース	子リソース
APP_IP	APP_NIC_Proxy
APP_CSManager	APP_IP

リソースをリンクするには、次の手順に従います。

a. 親リソースを右クリックし、[Link] を選択します。

[Link Resources] ダイアログボックスが表示されます。

b. 子リソースを選択し、[OK] をクリックします。

選択したリソースがリンクされます。

クラスタ レベル設定の作成

クラスタ レベル設定を作成するには、次の手順に従います。

ステップ 1　APPrep サービス グループの親として APP サービス グループをオンライン ローカル ファーム依存関係にリンクします。プライマリ クラスタとセカンダリ クラスタの両方でこの手順を実行します。

ステップ 2　クラスタ プロパティで、VCS_IP リソースで使用したのと同じ IP アドレスであるクラスタ アドレスを指定します。

ステップ 3　プライマリ クラスタから、[Edit] > [Add/Delete Remote Cluster] を選択して、リモート クラスタ設定ウィザードでセカンダリ クラスタを追加します。

ステップ 4　プライマリ クラスタから、[Edit] > [Configure Global Groups] を選択して、グローバル グループ設定ウィザードで APP サービス グループをグローバル グループとして設定します。

図 A-5（P.A-4）を参照してください。

CHAPTER 4

メンテナンス作業

この章では、HA/DR 構成で使用される Security Manager に関連するメンテナンス作業について説明します。この章は、次の内容で構成されています。

- 「VCS 動作のカスタマイズ」（P.4-1）
- 「SSL 用のセキュリティ証明書」（P.4-2）
- 「Security Manager の手動での起動、停止、またはフェールオーバー」（P.4-3）
- 「Cisco Secure ACS と Security Manager の統合」（P.4-6）
- 「Security Manager のアップグレード」（P.4-6）
- 「Security Manager のバックアップ」（P.4-7）
- 「Security Manager のアンインストール」（P.4-7）
- 「HA への非 HA Security Manager の移行」（P.4-8）

VCS 動作のカスタマイズ

VCS では、リソース障害への対応など、VCS 動作を制御するための大量の変数をサポートします。ここでは、このマニュアルの説明に従ってデフォルト インストールを行った場合のフェールオーバー動作の一部を示します。『*Veritas Cluster Server のガイド*』の説明に従って、このような動作の制御を確認する必要があります。

- Security Manager が失敗すると、VCS は同じサーバ上でアプリケーションを再起動しようとしません。代わりに、VCS は、クラスタ内のスタンバイ サーバにフェールオーバーします。ただし、リソースレベル属性 RestartLimit を使用して、エージェントがリソースの障害状態として宣言する前にリソースを再起動しようとする回数を制御できます。
- 特定のサーバで最初に Security Manager アプリケーションをオンラインにしようとすると、VCS はリソースを一度だけオンラインにしようとします。OnlineRetryLimit リソースレベル属性では、最初の試行が失敗した場合にオンライン エントリ ポイントを再試行する回数を指定します。
- デフォルトでは、VCS は 60 秒ごとに Security Manager アプリケーション モニタ スクリプトを実行します。これは、アプリケーションの障害を検出するのに最大 60 秒かかる可能性があることを意味します。MonitorInterval は調整できるリソースレベル属性です。
- デュアル クラスタを使用する場合、クラスタ間のフェールオーバーは、デフォルトでは手動操作です。これは、両方のクラスタで同時にアプリケーションを実行するのを回避します。クラスタ間の通信が失われた場合（冗長パスが地理的に離れたデータセンター間にない場合に発生しやすくなります）、VCS はリモート クラスタに障害が発生したかどうか、または通信に問題があるかどうかを判断できません。クラスタ間の自動フェールオーバーが必要な場合は、APP サービス グループの ClusterFailOverPolicy 属性で設定できます。

SSL 用のセキュリティ証明書

Security Manager では、サーバおよびクライアント ブラウザまたはアプリケーション間における Secure Socket Layer（SSL）の暗号化の使用を設定できます。SSL 暗号化には、サーバにおけるデジタル証明書の作成と配置が必要です。デジタル証明書に含まれている ID 情報の一部は、Common Services Web GUI に表示される Common Name（CN）または「Host Name」です。複数のサーバおよび対応するホスト名が存在する HA/DR 構成では、アプリケーションへのアクセスに使用されるホスト名または IP アドレスに一致する証明書を保持するために、特別な手順が必要になることがあります。

シングル クラスタの場合、単一の仮想 IP アドレスまたは仮想ホスト名でアプリケーションにアクセスします。この場合は、仮想 IP アドレスまたは仮想ホスト名と同じ CN で証明書を作成する必要があります。仮想 IP または仮想ホスト名のアドレスはアプリケーションを実行するクラスタ内のサーバに関係なく有効であるため、フェールオーバーの発生時にデジタル証明書ファイルを更新する必要はありません。

ただし、デュアル地理的クラスタ構成の場合、各クラスタにアプリケーションに関連付けられた独自の IP アドレスまたはホスト名があります。そのため、デジタル証明書ファイルがあるクラスタと一致するように作成されている場合、アプリケーションが他のクラスタにフェールオーバーすると一致しなくなります。この場合は、クラスタ間のフェールオーバーの発生時に、他のクラスタに一致するようにデジタル証明書ファイルを更新する必要があります。

（注） アプリケーションにアクセスするために仮想ホスト名を使用する場合は、代わりに DNS 更新を使用すると、クラスタ間フェールオーバーのために証明書を更新する必要がなくなります。クラスタ間フェールオーバーが発生すると、DNS は仮想ホスト名に関連付けられた新しい IP アドレスで更新されます。クライアントは常に同じ仮想ホスト名を使用してアプリケーションにアクセスするため、証明書ファイルを更新する必要はありません。

VCS 用の Security Manager エージェントは、アプリケーションを開始する前に非共有の複製されていないローカル ディレクトリに保存されているデジタル証明書ファイルを自動的にコピーできます。ただし、クラスタ内の各サーバでこのディレクトリに適切なファイルを配置する必要があります。ディレクトリは CertificateDir パラメータを使用してエージェントに指定されます。

各サイトにサーバが 1 台ある地理的冗長性（DR）構成の場合は、よりシンプルなオプションを使用できます。サーバのホスト名に基づいて証明書ファイルを再生成するようにエージェントを設定できます。これは、仮想 IP アドレスまたは仮想ホスト名がないため動作します。エージェントをこのように動作するように設定するには、CertificateDir パラメータの値にキーワード **regen** を指定します。

Security Manager をインストールすると、サーバのローカル ホスト名に一致する自己署名証明書がデフォルトで作成されます。構成に応じて、仮想 IP アドレスまたは仮想ホスト名に一致する自己署名証明書を生成するには、次の手順に従います。

ステップ 1　サーバ（http://<*hostname or IP address*>:1741）の Web ブラウザ インターフェイスにログインします。

ステップ 2　次のように自己署名証明書セットアップ画面にアクセスします。

a. Cisco Security Management Suite のホームページで、[Server Administration] をクリックします。

b. [Server Admin] ページのメニューから、[Server] > [Single Server Management] > [Certificate Setup] を選択します。

ステップ 3　証明書のフィールドに入力し、[CN] フィールドで仮想 IP アドレスまたは仮想ホスト名を指定し、[Apply] をクリックします。

次の証明書関連ファイルは、NMSROOT\MDC\Apache\conf\ssl ディレクトリに生成されます。

- server.key

- server.crt
- server.pk8
- server.csr
- openssl.conf
- chain.cer

シングル クラスタを使用する場合は、これ以上の処理は必要ありません。ただし、各クラスタ内に複数のサーバが配置されたデュアル地理的クラスタ構成を使用する場合は、クラスタ内の各サーバでこれらの証明書関連ファイルを非共有の複製されていないローカル ディレクトリにコピーする必要があります。次に、セカンダリ クラスタに対して同じ手順を実行します。ただし、今度はセカンダリ クラスタの仮想 IP アドレスまたは仮想ホスト名を指定します。CSManager リソースを定義する場合、選択された非共有の複製されていないローカル ディレクトリを **CertificateDir** 属性に指定します。エージェントは、フェールオーバー後、アプリケーションを開始する前に適切な作業ディレクトリに自動的に証明書ファイルをコピーします。

Security Manager の手動での起動、停止、またはフェールオーバー

非 HA/DR 構成では、通常、Windows Services アプリケーションまたはコマンドラインのそれに相当する **net start** および **net stop** を使用して Security Manager を起動および停止します。ただし、HA/DR 構成では、この方法を使用しないでください。HA/DR 構成では、Security Manager を起動および停止するための特定のスクリプトが提供されています。これらのスクリプトでは、異なるサーバで Security Manager を起動する場合に必要な追加手順を実行します。これらのスクリプトおよびその他のスクリプトは VCS 用の Security Manager エージェントを構成します。エージェントを使用すると、VCS で Security Manager を制御およびモニタできます。VCS を使用しない場合は、これらのスクリプトを使用して、Security Manager を手動で起動および停止できます。

ここでは、次の内容について説明します。

- 「VCS の場合」（P.4-3）
- 「VCS 以外の場合」（P.4-4）

VCS の場合

VCS を使用する場合、VCS コントロールを使用して、Security Manager サービス グループ（APP）を手動で起動、停止、およびフェールオーバーする必要があります。VCS 用語では、起動および停止はそれぞれオンラインおよびオフラインと呼ばれます。VCS GUI または VCS コマンドライン インターフェイスを使用して、Security Manager サービス グループをオンラインにしたり、オフラインにしたり、フェールオーバーしたりできます。付録 B「ハイ アベイラビリティおよびディザスタ リカバリ証明テスト計画」（P.B-1）に、このような操作の実行例があります。

注意　VCS の外部で Security Manager を手動で（net stop を使用するなどして）を停止すると、VCS はこれをアプリケーション障害として認識し、リカバリの開始を試行します。

VCS 以外の場合

VCS を使用しない場合は、Security Manager に付属の **online** および **offline** スクリプトを使用して Security Manager を起動および停止できます。これらのスクリプトは次の場所にあります。

$NMSROOT\MDC\athena\ha\agent（Veritas 5.1 SP1 用）

$NMSROOT\MDC\athena\ha\agent\Veritas60（Veritas 6.0 用）

Veritas 5.1 SP1 用の Windows Server 2008 の構文：

```
perl online.pl CSManager PathName 1 <PathName>  EventIPAddress 1 <EventIPAddress>
[ CertificateDir 1 <CertificateDir>|regen ]
```

例：

```
perl online.pl CSManager PathName 1 F:\Progra~1\CSCOpx EventIPAddress 1 10.76.10.238
```

（注） コマンド プロンプトを開くときに [Run as administrator] オプションを選択する必要があります。

Veritas 6.0 用の Windows Server 2008 の構文：

```
perl online.pl CSManager <PathName> <EventIPAddress> [ <CertificateDir>|regen ]
```

例：

```
perl online.pl CSManager F:\Progra~1\CSCOpx 10.76.10.238
```

（注） コマンド プロンプトを開くときに [Run as administrator] オプションを選択する必要があります。

構文	説明
<PathName>	Security Manager のインストール パス（たとえば、「F:\Program Files\CSCOpx」）。インストール パスにスペースが含まれる場合、引用符で引数を囲みます。
<EventIPAddress>	Security Manager アプリケーションがクライアント/サーバとサーバ/デバイスの通信に使用する IP アドレス。
<CertificateDir>	任意。SSL 証明書ファイルが保管される、非共有の複製されていないローカル ディレクトリを指定できます。指定した場合、スクリプトは、アプリケーションが使用するインストール ディレクトリの下の適切なディレクトリにこれらのファイルをコピーします。**regen** キーワードが使用されている場合、スクリプトは、サーバのローカル ホスト名に基づいて SSL 証明書を再生成します。このパラメータに使用される値に関係なく、サーバのホスト名が Security Manager アプリケーション ファイルのホスト名と一致する場合は、証明書に対して行う処理はありません。「SSL 用のセキュリティ証明書」（P.4-2）も参照してください。

Windows Server 2008 用の **offline** スクリプトの構文は次のとおりです。

Veritas 5.1 用の Windows Server 2008 の構文：

```
perl offline.pl CSManager PathName 1 <PathName>
```

例：

```
perl offline.pl CSManager PathName 1 F:\Progra~1\CSCOpx
```

（注） コマンド プロンプトを開くときに [Run as administrator] オプションを選択する必要があります。

Veritas 6.0 用の Windows Server 2008 の構文：

```
perl offline.pl CSManager <PathName>
```

例：

```
perl offline.pl CSManager F:\Progra~1\CSCOpx
```

（注） コマンド プロンプトを開くときに [Run as administrator] オプションを選択する必要があります。

構文	説明
PathName	Security Manager のインストール パス（たとえば、「F:\Program Files\CSCOpx」）。インストール パスにスペースが含まれる場合、引用符で引数を囲みます。

使いやすさのために、構成に適した属性を含むオンラインおよびオフライン バッチ ファイル（online.bat、offline.bat など）を作成する必要がある場合があります。

手動フェールオーバーを実行するには、VEA またはコマンドラインを使用して、複製されたボリューム グループ内でプライマリ ロールを転送できます。プライマリ サーバとセカンダリ サーバの両方が動作している場合、プライマリ ロールをセカンダリに移行（複製の方向を効果的に逆に）できます。または、プライマリ サーバに障害が発生して使用できない場合は、（高速フェールバックの有無に関係なく）セカンダリ サーバにプライマリ ロールを引き継がせることができます。詳細については、『Veritas Volume Replicator administrator's guide』を参照してください。

次は、2 台のサーバ間で複製を使用するディザスタ リカバリ構成の手動フェールオーバー手順の概要です。

ステップ 1　offline.pl スクリプトを使用してプライマリ サーバで Security Manager を停止します。

ステップ 2　プライマリ サーバ上の Security Manager に使用されるボリュームのドライブ文字の割り当てを解除します。

ステップ 3　VEA GUI を使用してプライマリ サーバからセカンダリ サーバに所有権を移行します。

ステップ 4　セカンダリ サーバの Security Manager に使用されるボリュームにドライブ文字を割り当てます。

ステップ 5　online.pl スクリプトを使用してセカンダリ サーバの Security Manager を起動します。

（注）　セカンダリ サーバへの移行またはフェールオーバーが初めての場合、casusers グループのファイル権限をアップグレードする必要があります。これは、ワンタイム アクティビティです。詳細については、「作業ボリュームに対する権限の更新」（P.3-14）を参照してください。

Cisco Secure ACS と Security Manager の統合

『*Installation Guide for Cisco Security Manager*』で説明されているように、Cisco Secure ACS を Security Manager に統合して、Security Manager ユーザに高度な許可を付与できます。HA/DR 構成では、ACS の AAA クライアントとして設定に関連する各 Security Manager サーバを追加する必要があります。ACS でサーバを指定した場合、サーバの物理ホスト名に関連付けられた固定 IP アドレスを指定します。

ACS 統合で Security Manager に HA/DR 構成を使用する場合は、複数の ACS サーバを展開して、ACS がシングル ポイント障害になるのを回避する必要もあります。ACS サーバが 1 台だけあり、そのサーバで障害が発生した場合は、修正措置を行って ACS を復元するかローカル認証を使用するように Security Manager サーバをリセットしなければ、Security Manager にログインできません。ACS は、プライマリ ACS とのセカンダリ ACS の同期を維持するためにデータベース複製が使用される、プライマリ ACS と複数のセカンダリ ACS の展開をサポートします。Security Manager では、最大 3 つの ACS の指定をサポートするため、最初の ACS が使用できない場合は、必要に応じて 2 台目を試行し、最後に 3 台目を試行します。

Security Manager のアップグレード

Security Manager のアップグレードには、さまざまな形態があります。

- メジャー リリース（リリースの最初の数字の変更。たとえば、3.x から 4.x に変更）
- マイナー リリース（リリースの 2 桁目の数字の変更。たとえば、3.1 から 3.2 に変更）
- メンテナンス リリース（リリースの 3 桁目の数字の変更。たとえば、3.1 から 3.1.1 に変更）
- サービス パック（Security Manager 3.1 用の SP2 など、サービス パック ID で識別される）

HA/DR 構成の Security Manager をアップグレードする場合、主な違いは、Security Manager のアクティブ インスタンスでプライマリ サーバのみをアップグレードする必要があるのか、または Security Manager をサーバ上で実行するために必要な正しいレジストリ設定を行うために、Security Manager のスペア コピーのみが存在するセカンダリ サーバもアップグレードする必要があるかということです。アップグレードによってレジストリが変更される場合、HA/DR 構成のすべてのサーバでアップグレードを実行する必要があります。通常、サービス パックはレジストリに影響しないため、プライマリ サーバだけにサービス パックをインストールするだけで十分です。メジャー、マイナー、またはメンテナンス リリースでは、通常、すべてのサーバをアップグレードする必要があります。ただし、readme ファイルまたはリリース ノートでこれらのガイドラインの例外を確認してください。

セカンダリ サーバをアップグレードする場合は、Security Manager サーバのスペア コピーを構成内のすべてのサーバで使用される標準の $NMSROOT（F:\Program Files\CSCOpx など）パスにマウントして、定期的なアップグレードをインストールする必要があります。これにより、セカンダリ サーバで Security Manager のアップグレード バージョンを実行するために正しいレジストリ設定が行われます。

アップグレードする前に、すべてのサーバで VCS を停止します（クラスタ内の任意のサーバで **hastop -all -force** を使用すると、クラスタ内のすべてのサーバで VCS が停止し、アプリケーションとリソースは動作可能なままになります）。すべてのサーバでアップグレードし、構成で複製が使用されている場合は、アップグレード時に複製を一時停止するか停止し、アップグレードの完了後にセカンダリ サーバを同期する必要があります。

Security Manager のバックアップ

Security Manager の HA/DR 展開構成によって、Security Manager の定期的なバックアップが不要になるわけではありません。HA/DR 構成により、ハードウェア障害によるデータ損失やアプリケーションのダウンタイムから保護されます。ただし、Security Manager に保持されている重要な情報を誤って、または悪意を持って変更または削除されるなどのユーザ アクションからは保護されません。したがって、Security Manager データベースおよび情報ファイルを引き続きバック アップする必要があります。Security Manager のバック アップ機能を使用できます。

セカンダリ サーバに関連付けられているスペア インスタンスではなく、Security Manager のプライマリ アクティブ インスタンスのみをバックアップする必要があります。Security Manager は、HA/DR 構成内のサーバまたは互換性のある Security Manager アプリケーションがインストールされているサーバで復元できます。

Security Manager のアンインストール

HA/DR 構成のすべてのサーバから Security Manager をアンインストールするには、次の手順に従います。

ステップ 1　プライマリ クラスタ内のプライマリ サーバで Security Manager が実行されていることを確認します。

ステップ 2　Cluster Explorer を使用して、**APP_CSManager** リソースを右クリックし、[critical] チェックボックスをオフにします。読み取り / 書き込みモードに切り替えるよう求められるため、このダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 3　**APP_CSManager** リソースを右クリックし、プライマリ サーバで [Offline] を選択します。Security Manager がオフラインになるまで待ちます。

ステップ 4　APP_CSManager リソースを削除し、VCS 設定を保存します。

ステップ 5　複製を利用する場合は、VEA GUI を使用して複製を停止します。

ステップ 6　プライマリ サーバで Security Manager をアンインストールするには、[Start] > [All Programs] > [Cisco Security Manager] > [Uninstall Cisco Security Manager] を選択します。

ステップ 7　セカンダリ サーバで、VEA GUI またはコマンドラインを使用して、cscopx_spare ボリュームを含むディスク グループをインポートします（まだインポートしていない場合）。

ステップ 8　VEA GUI またはコマンドラインを使用して、cscopx_spare ボリュームに選択したドライブ文字を割り当てます。

ステップ 9　プライマリ サーバで Security Manager をアンインストールするには、[Start] > [All Programs] > [Cisco Security Manager] > [Uninstall Cisco Security Manager] を選択します。

ステップ 10　他のセカンダリ サーバまたはセカンダリ クラスタ内のプライマリ サーバでステップ 7 ～ 9 を繰り返します。

（注）　Security Manager を再インストールする予定がない場合は、Security Manager に関連付けられた VCS 内のサービス グループおよび複製を使用している場合は複製されたボリューム グループを削除する必要があります。不要なボリュームおよびディスク グループも削除する必要があります。

HA への非 HA Security Manager の移行

通常の非 HA 構成に既存の Security Manager がインストールされている場合は、この項で HA 構成にそのインスタンスを移行する方法について説明します。移行を実行するには、次の手順を使用します。

ステップ 1　『*User Guide for CiscoWorks Common Services 3.2*』の説明に従って、既存の Security Manager インスタンスのバックアップを実行します。次の URL にある「*Configuring the Server*」という章の「*Backing* Up Data」という項を参照してください。
http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_common_services_software/3.2/user/guide/admin.html

ステップ 2　このマニュアルの説明に従って、目的の Security Manager HA または DR 導入環境を作成します。

ステップ 3　『*User Guide for CiscoWorks Common Services 3.2*』の説明に従って、元の Security Manager インスタンスから作成したバックアップを HA または DR 導入環境のプライマリ サーバに復元します。上記のリンクにある「Restoring Data」という項を参照してください。

ステップ 4　セカンダリ サーバのレジストリ内のデータベース パスワードをプライマリ サーバのパスワードと手動で同期します。プライマリ サーバで、レジストリ エディタ（[Start] > [Run] > [regedit]）を使用して、HKEY_LOCAL_MACHINE\SOFTWARE\OBDC\OBDC.INI の cmf、vms、rmeng フォルダにある CWEPWD エントリの値を探して書き留めます。セカンダリ マシンの CWEPWD レジストリ値をプライマリの値と一致するように編集します。

APPENDIX A

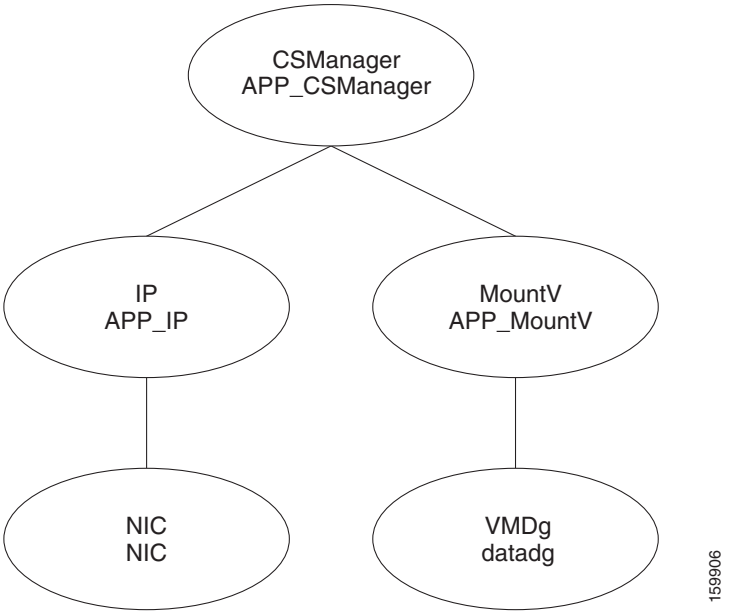
参照構成の VCS リソース ビュー

ここでは、このマニュアルで説明されている HA/DR Security Manager 構成の Veritas Cluster Server（VCS）リソース ビューとサービス グループ ビューに関する情報を提供します。図 A-1 ～図 A-5 に、サービス グループのリソース間の依存関係およびサービス グループ間の依存関係を示します。この図では、2 つのリソース間の線は、依存関係、つまり親子関係を表します。リソースの依存関係は、リソースをオンラインおよびオフラインにする順序を指定します。フェールオーバー中は、図の上部に最も近いリソースをオフラインにする必要があり、その後、そのリソースにリンクされているリソースがオフラインになります。同様に、図の下部に最も近いリソースをオンラインにする必要があり、その後、そのリソースにリンクされているリソースをオンラインになります。他のリソースに依存するリソースは親リソースです。図では、親リソースのアイコンをその下にある子リソースのアイコンにリンクしています。

シングル ローカル クラスタ（デュアル ノード）構成

図 A-1 に、クラスタ内に 2 台のサーバを持つシングル クラスタの Veritas Cluster Server（VCS）リソース ビューを示します。

図 A-1　リソース ビュー : APP グループ（シングル クラスタ、デュアル ノード）



デュアル地理的クラスタ（シングル ノード）構成

図 A-2 ～図 A-5 に、クラスタ内に 1 台のサーバを持つデュアル クラスタ構成の Veritas Cluster Server（VCS）リソース ビューを示します。

図 A-2　リソース ビュー : APP グループ（デュアル クラスタ、シングル ノード）

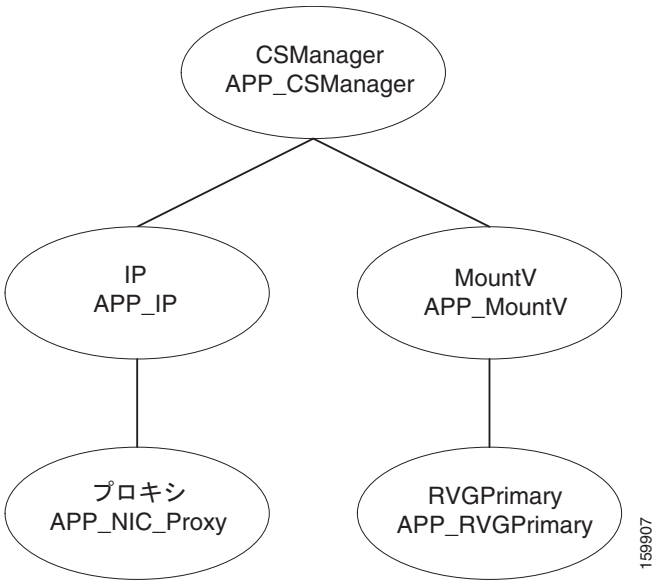


図 A-3　リソース ビュー : APPrep グループ（デュアル クラスタ、シングル ノード）

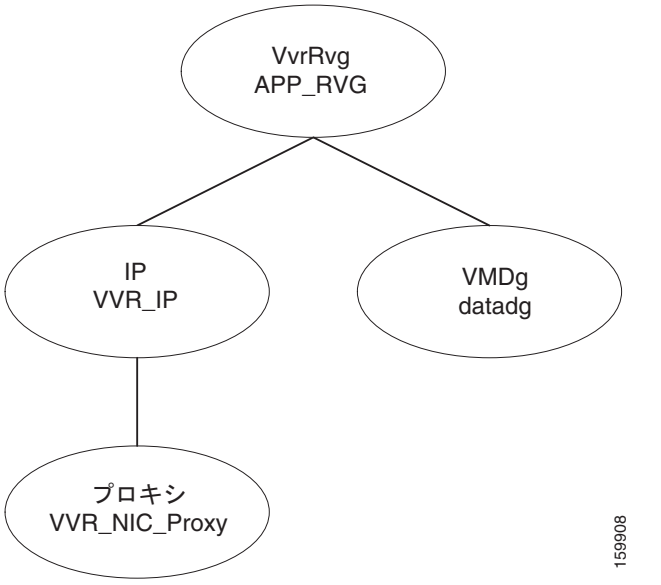


図 A-4　リソース ビュー : ClusterService グループ（デュアル クラスタ、シングル ノード）

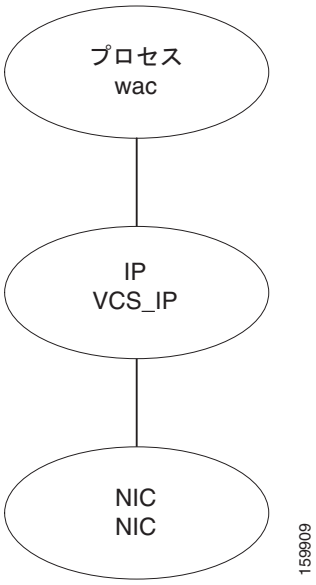
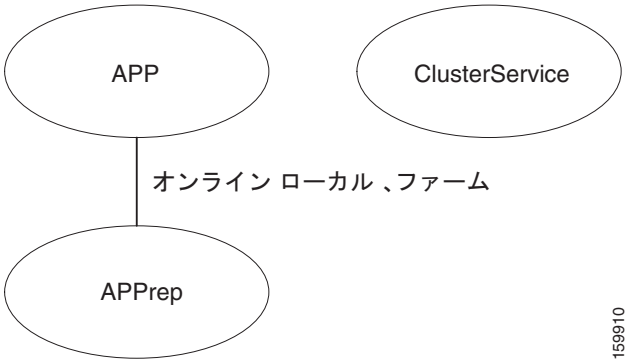


図 A-5　サービス グループ ビュー（デュアル クラスタ、シングル ノード）



APPENDIX B

ハイ アベイラビリティおよびディザスタ リカバリ証明テスト計画

HA/DR 証明テスト計画では、Security Manager アプリケーションが高いアベイラビリティを備え、さまざまなハードウェア障害やソフトウェア障害に対応できることを検証します。テスト計画には、サーバ間でのアプリケーションの手動切り替えなど、メンテナンス作業も含まれます。

（注） Security Manager クライアント セッションでは、アクティブ ユーザがアプリケーションのフェールオーバー後に再度ログインする必要があります。この動作は、サーバで実行されている Security Manager サービスの停止および開始と同じです。

この付録には、次のテスト ケース カテゴリがあります。

- 「手動切り替え」（P.B-1）
- 「イーサネット/ネットワーク障害」（P.B-3）
- 「サーバの障害」（P.B-10）
- 「アプリケーションの障害」（P.B-16）

手動切り替え

ここでは、2 種類の手動切り替えについて説明します。2 台のサーバを持つシングル クラスタでは、クラスタ内で 2 台のサーバを切り替えることができます（クラスタ内切り替え）。各クラスタ内に 1 台のサーバが配置されたデュアル クラスタ構成では、クラスタを切り替えることができます（クラスタ間切り替え）。

ここでは、次の項目について説明します。

- 「クラスタ内切り替え」（P.B-1）
- 「クラスタ間切り替え」（P.B-2）

クラスタ内切り替え

テスト ケース タイトル：クラスタ内の手動アプリケーション切り替え。

説明：アプリケーションは、VCS を使用して、同じクラスタ内の別のサーバに手動で切り替えられます。

テスト セットアップ：シングル クラスタ構成内のデュアル ノード クラスタ（図 1-1（P.12））。

ステップ 1　APP サービス グループがプライマリ サーバで実行されていることを確認します。VCS Cluster Explorer を使用して、[APP] サービス グループを選択します。ショートカット メニューから [Switch To] を選択し、セカンダリ サーバを選択します。または、次のコマンドを発行します。

```
C:\> hagrp -switch APP -to secondary_server_name
```

ステップ 2　APP サービス グループのリソース ビューで、サービス グループのリソースがプライマリ サーバでオフラインになり、その後セカンダリ サーバでオンラインになることを確認します。または、次のコマンドを発行して、APP サービス グループのステータスを確認します。

```
C:\> hagrp -state APP
```

ステップ 3　クライアント マシンから、ログイン ダイアログボックスで [Server Name] フィールドに仮想ホスト名または IP アドレスを使用して Security Manager クライアントを起動します。アプリケーションに正常にログインできることを確認します。

クラスタ間切り替え

テスト ケース タイトル: クラスタ間の手動アプリケーション切り替え。

説明: アプリケーションは、VCS を使用して、異なるクラスタ内のサーバに手動で切り替えられます。

テスト セットアップ: 各クラスタ内に 1 台のサーバが配置された、図 1-2（P.14）に示すデュアル クラスタ構成。

ステップ 1　VCS Cluster Explorer を使用して、[APP] サービス グループを選択します。ショートカット メニューから、[Switch To]、[Remote Switch(...)] の順に選択して [Switch global] ダイアログボックスを開きます。ダイアログボックスで、リモート クラスタと、必要に応じてリモート クラスタ内の特定のサーバを指定します。または、次のコマンドを発行します。

```
C:\> hagrp -switch APP -any -clus secondary_cluster_name
```

ステップ 2　APP サービス グループのリソース ビューで、サービス グループのリソースがプライマリ クラスタでオフラインになることを確認します。ツリーでルート クラスタ ノードを選択し、[Remote Cluster Status] ビューを使用して、APP サービス グループがリモート クラスタでオンラインになることを確認します。または、次のコマンドを発行して、APP サービス グループのステータスを確認します。

```
C:\> hagrp -state APP
#Group       Attribute            System                        Value
APP          State                csm_primary:<Primary Server>  |OFFLINE|
APP          State                localclus:<Secondary Server>  |ONLINE|
```

ステップ 3　クライアント マシンから、ログイン ダイアログボックスで [Server Name] フィールドにセカンダリ クラスタで使用されている適切なホスト名またはアプリケーション IP アドレスを入力して Security Manager クライアントを起動します。アプリケーションに正常にログインできることを確認します。

ステップ 4　Security Manager クライアントからログアウトし、VCS Cluster Explorer または次のコマンドを使用して、APP サービス グループをプライマリ クラスタに切り替えます。

```
C:\> hagrp -switch APP -any -clus primary_cluster_name
```

イーサネット/ネットワーク障害

HA/DR 構成には、2 つのタイプのサーバ イーサネット接続があります。1 つ目はネットワーク通信に使用されるイーサネット接続です（パブリック インターフェイス）。2 つ目は、クラスタ内通信専用のイーサネット インターフェイスです（プライベート インターフェイス）。ここでは、イーサネット インターフェイスの各タイプの障害テスト ケースについて説明します。

- 「ネットワーク通信障害」（P.B-3）
- 「クラスタ通信障害」（P.B-8）

ネットワーク通信障害

ここでは、VCS がネットワーク通信に使用されているネットワーク イーサネット ポートの障害を検出できることを確認するために使用するテストを示します。ここでは、次の項目について説明します。

- 「セカンダリ サーバ、シングル クラスタにおけるネットワーク イーサネット障害」（P.B-3）
- 「プライマリ サーバ、シングル クラスタにおけるネットワーク イーサネット障害」（P.B-4）
- 「セカンダリ サーバ、デュアル クラスタにおけるネットワーク イーサネット障害」（P.B-5）
- 「プライマリ サーバ、デュアル クラスタにおけるネットワーク イーサネット障害」（P.B-7）

セカンダリ サーバ、シングル クラスタにおけるネットワーク イーサネット障害

テスト ケース タイトル：シングル クラスタ構成内のセカンダリ サーバのネットワーク イーサネット接続で障害が発生しました。

説明：このテスト ケースでは、VCS がセカンダリ サーバのネットワーク イーサネット ポートの障害を検出し、障害の修復後に回復できることを確認します。

テスト セットアップ：サーバごとに 1 本のネットワーク接続を備えたシングル クラスタ構成内のデュアル ノード クラスタ（図 1-1（P.12））。

ステップ 1　アプリケーションがプライマリ サーバで実行されていることを確認します。

ステップ 2　クライアント マシンからアプリケーションにログインします。

ステップ 3　セカンダリ サーバのネットワーク ポートからイーサネット ケーブルを取り外して、スイッチ/ルータ ネットワークとの通信からサーバを分離します。VCS がネットワーク ポート障害を検出するまで少なくとも 60 秒間待機します。次のコマンドを実行して、VCS がセカンダリ サーバの NIC リソースの障害を検出することを確認します。

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A <PrimaryServer>       RUNNING              0
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               ONLINE
B  APP             <SecondaryServer>    Y          N               OFFLINE|FAULTED

-- RESOURCES FAILED
-- Group           Type                 Resource             System
C  APP             NIC                  NIC                  <SecondaryServer>
```

ステップ 4　セカンダリ サーバのネットワーク ポートにイーサネット ケーブルを戻します。次のコマンドを実行して、障害の解消を VCS が検出することを確認します。

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               ONLINE
B  APP             <SecondaryServer>    Y          N               OFFLINE
```

プライマリ サーバ、シングル クラスタにおけるネットワーク イーサネット障害

テスト ケース タイトル: シングル クラスタ構成内のプライマリ サーバのネットワーク イーサネット接続で障害が発生しました。

説明: このテスト ケースでは、VCS がプライマリ サーバのネットワーク イーサネット ポートの障害を検出し、アプリケーションを自動的にセカンダリ サーバに切り替えることができることを確認します。問題が修正された後、アプリケーションを再びプライマリ サーバに手動で切り替えるできます。

テスト セットアップ: サーバごとに 1 本のネットワーク接続を備えたデュアル ノード クラスタ（図 2-2（P.23））。

ステップ 1　アプリケーションがプライマリ サーバで実行されていることを確認します。

ステップ 2　プライマリ サーバのネットワーク ポートからイーサネット ケーブルを取り外して、スイッチ/ルータ ネットワークとの通信からサーバを分離します。VCS が NIC リソースの障害を検出し、自動的にセカンダリ サーバに APP サービス グループを切り替えることを確認します。

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               OFFLINE|FAULTED
B  APP             <SecondaryServer>    Y          N               ONLINE

-- RESOURCES FAILED
-- Group           Type                 Resource             System
C  APP             NIC                  NIC                  <PrimaryServer>
C  APP             IP                   APP_IP               <PrimaryServer>
```

ステップ 3　セカンダリ サーバで実行中のアプリケーションにログインできることを確認します。

ステップ 4　プライマリ サーバのネットワーク ポートのイーサネット ケーブルを交換し、プライマリ サーバの障害が発生している IP リソースを手動でクリアします。

```
C:\> hares -clear APP_IP -sys primary_server_name
```

ステップ 5　APP サービス グループを再びプライマリ サーバに手動で切り替えます。

```
C:\> hagrp -switch APP -to primary_server_name
```

セカンダリ サーバ、デュアル クラスタにおけるネットワーク イーサネット障害

テスト ケース タイトル: デュアル クラスタ構成内のセカンダリ サーバのネットワーク イーサネット接続で障害が発生しました。

説明: このテスト ケースでは、VCS がネットワーク イーサネット ポートの障害を検出し、障害の修復後に回復できることを確認します。

テスト セットアップ: クラスタごとにシングル ノード、およびサーバごとに 1 本のイーサネット ネットワーク接続を備えたデュアル クラスタ構成（図 1-2（P.14））。

ステップ 1　APP サービス グループがプライマリ クラスタ/サーバで実行されていることを確認します。

ステップ 2　クライアント マシンから Security Manager にログインします。

ステップ 3　セカンダリ クラスタ内のサーバのネットワーク ポートからイーサネット ケーブルを取り外します。これにより、スイッチ/ルータ ネットワークとの通信からサーバが分離され、複製が中断されます。プライマリ サーバで、次のコマンドを実行して、複製が中断（切断）されたことを確認します。

```
C:\> vxprint -Pl
Diskgroup = datadg

Rlink      : rlk_172_6037
info       : timeout=500 packet_size=1400
             latency_high_mark=10000 latency_low_mark=9950
             bandwidth_limit=none
state      : state=ACTIVE
             synchronous=off latencyprot=off srlprot=off
assoc      : rvg=CSM_RVG
             remote_host=172.25.84.34
             remote_dg=datadg
             remote_rlink=rlk_172_32481
             local_host=172.25.84.33
protocol   : UDP/IP
flags      : write attached consistent disconnected
```

ステップ 4　プライマリ サーバから次のコマンドを実行して、セカンダリ クラスタとの通信が失われたことを確認します。

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               ONLINE
B  APPrep          <PrimaryServer>      Y          N               ONLINE
B  ClusterService  <PrimaryServer>      Y          N               ONLINE

-- WAN HEARTBEAT STATE
-- Heartbeat       To                   State
L  Icmp            csm_secondary        ALIVE

-- REMOTE CLUSTER STATE
-- Cluster         State
M  csm_secondary   LOST_CONN
```

```
-- REMOTE SYSTEM STATE
-- cluster:system                    State                Frozen
N  csm_secondary:<SecondaryServer>   RUNNING              0

-- REMOTE GROUP STATE
-- Group           cluster:system       Probed     AutoDisabled    State
O  APP csm_secondary:<SecondaryServer>  Y          N               OFFLINE
```

ステップ 5　ネットワーク イーサネット ケーブルをセカンダリ サーバに再接続し、複製が再開されたことを確認します。

```
C:\> vxprint -Pl

Diskgroup = datadg

Rlink      : rlk_172_6037
info       : timeout=29 packet_size=1400
             latency_high_mark=10000 latency_low_mark=9950
             bandwidth_limit=none
state      : state=ACTIVE
             synchronous=off latencyprot=off srlprot=off
assoc      : rvg=CSM_RVG
             remote_host=172.25.84.34
             remote_dg=datadg
             remote_rlink=rlk_172_32481
             local_host=172.25.84.33
protocol   : UDP/IP
flags      : write attached consistent connected
```

ステップ 6　セカンダリ クラスタへの通信が復元されたことを確認します。

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0
-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               ONLINE
B  APPrep          <PrimaryServer>      Y          N               ONLINE
B  ClusterService  <PrimaryServer>      Y          N               ONLINE

-- WAN HEARTBEAT STATE
-- Heartbeat       To                   State
L  Icmp            csm_secondary        ALIVE

-- REMOTE CLUSTER STATE
-- Cluster         State
M  csm_secondary   RUNNING

-- REMOTE SYSTEM STATE
-- cluster:system                    State                Frozen
N  csm_secondary:<SecondaryServer>   RUNNING              0

-- REMOTE GROUP STATE
-- Group           cluster:system       Probed     AutoDisabled    State
O  APP csm_secondary:<SecondaryServer>  Y          N               OFFLINE
```

ステップ 7　複製が回復しない場合は、次のように障害が発生した IP リソースを手動でクリアし、次にセカンダリで APPrep サービス グループを開始する必要があります。

```
C:\> hares -clear APP_IP
C:\> hagrp -online APPrep -sys secondary_server_name
```

プライマリ サーバ、デュアル クラスタにおけるネットワーク イーサネット障害

テスト ケース タイトル：プライマリ サーバのネットワーク イーサネット接続で障害が発生しました。

説明：このテスト ケースでは、VCS がプライマリ サーバのネットワーク イーサネット ポートの障害を検出し、セカンダリ サーバでアプリケーションを起動して回復できることを確認します。イーサネット接続の復元後、元のプライマリ サーバに手動でフェールオーバーし、セカンダリでの実行中に行われたデータ変更を保持します。

テスト セットアップ：各クラスタ内に 1 台のノードが配置されたデュアル クラスタ構成（図 1-2 (P.14)）。

ステップ 1　**APP** サービス グループがプライマリ クラスタで実行されていることを確認します。

ステップ 2　プライマリ クラスタ内のサーバのポートからイーサネット ケーブルを取り外して、スイッチ/ルータ ネットワークとの通信からサーバを分離します。VCS は、IP および NIC リソースの障害としてこれを検出する必要があります。VCS が障害を検出し、APP サービス グループを停止したことを確認します。

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A <PrimaryServer>       RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               OFFLINE
B  APPrep          <PrimaryServer>      Y          N               OFFLINE|FAULTED
B  ClusterService  <PrimaryServer>      Y          N               ONLINE

-- RESOURCES FAILED
-- Group           Type                 Resource             System
C  APPrep          IP                   APP_IP               <PrimaryServer>
C  APPrep          NIC                  NIC                  <PrimaryServer>

-- WAN HEARTBEAT STATE
-- Heartbeat       To                   State
L  Icmp            csm_secondary        DOWN

-- REMOTE CLUSTER STATE
-- Cluster         State
M  csm_secondary   FAULTED

-- REMOTE SYSTEM STATE
-- cluster:system       State                Frozen
N  csm_secondary:<SecondaryServer> FAULTED             0

-- REMOTE GROUP STATE
-- Group           cluster:system                  Probed     AutoDisabled    State
O  APP             csm_secondary:<SecondaryServer> Y          N               OFFLINE
```

ステップ 3　セカンダリ サーバで次のコマンドを使用して、セカンダリ クラスタの APP サービス グループを開始します。

```
C:\> hagrp -online -force APP -sys secondary_server_name
```

ステップ 4　クライアント マシンから、Security Manager にログインして Security Manager が動作していることを確認します。プライマリ サーバに切り替えたときに変更が維持されることを確認できるように、データを変更します。

ステップ 5　プライマリ クラスタ サーバにネットワーク イーサネット ケーブルを再接続します。

ステップ 6　IP リソースの障害を取り除き、プライマリ サーバから **APPrep** サービスをオンにします。

```
C:\> hares -clear APP_IP
C:\> hagrp -online APPrep -sys primary_server_name
```

ステップ 7　元のプライマリ RVG をセカンダリに変換し、高速フェールバック機能を使用して、元のプライマリ RVG のデータ ボリュームを新しいプライマリ RVG のデータ ボリュームと同期します。セカンダリ クラスタの Cluster Explorer を使用して、RVGPrimary リソース（**APP_RVGPrimary**）を右クリックし、[actions] を選択して [Actions] ダイアログボックスから [fbsync] を選択し、[OK] をクリックします。または、次のコマンドを発行できます。

```
C:\> hares -action APP_RVGPrimary fbsync 0 -sys secondary_server_name
```

ステップ 8　セカンダリ クラスタで VCS Cluster Explorer を使用して、[APP] サービス グループを選択します。ショートカット メニューから、[Switch To]、[Remote Switch(...)] の順に選択して [Switch global] ダイアログボックスを開きます。ダイアログボックスで、プライマリ クラスタとプライマリ サーバを指定します。または、次のコマンドを発行します。

```
C:\> hagrp -switch APP -any -clus primarycluster
```

ステップ 9　アプリケーションにログインして、セカンダリ サーバに加えた変更が保持されていることを確認します。

クラスタ通信障害

テスト ケース タイトル：クラスタ通信に使用されるイーサネットで障害が発生しました。

説明：クラスタ内通信のためにクラスタ内のサーバ間で使用されている専用のイーサネット接続で障害が発生しました。テストでは、3 本のうち最大 2 本の冗長通信パスが失われた場合でも、クラスタ通信が継続されることを確認します。

テスト セットアップ：2 本の専用クラスタ通信イーサネット接続、およびネットワーク イーサネット接続に設定されたプライオリティの低いクラスタ通信接続を備えた、シングル クラスタ構成のデュアル ノード クラスタ（図 1-1（P.12））。

（注）　このテスト ケースで指定されたコマンドに加えて、Cluster Explorer からツリーでルート ノードを選択し、[System Connectivity] タブを選択することによってクラスタ通信のステータスをモニタできます。

ステップ 1　次のコマンドを発行して、すべてのシステムが GAB を介して通信していることを確認します。

（注）　Group Membership Services/Atomic Broadcast（GAB）は、クラスタ メンバーシップやクラスタ通信を担当する VCS プロトコルです。

```
# gabconfig -a
GAB Port Memberships
===============================================================
Port a gen   e8cc02 membership 01
```

```
Port h gen   e8cc01 membership 01
```

ステップ 2　プライマリ サーバでクラスタ通信に使用される最初の専用イーサネット ポートからイーサネット ケーブルを取り外します。

ステップ 3　次のコマンドを発行して、クラスタ通信に使用されるリンクの詳細なステータスを表示し、最初の専用クラスタ通信ポートがダウンしていることを確認します。

（注）　出力のアスタリスク（*）は、コマンドが実行されるサーバを示します。コマンドが実行されるサーバは、これらのポートの 1 つ以上が物理的に切断されている場合でも、常にリンクがアップしていることを示します。

```
# lltstat -nvv
LLT node information:
    Node           State    Link  Status  Address
   * 0 <PrimaryServer>   OPEN
                                Adapter0   UP    00:14:5E:28:52:9C
                                Adapter1   UP    00:14:5E:28:52:9D
                                Adapter2   UP    00:0E:0C:9C:20:FE
     1 <SecondaryServer> OPEN
                                Adapter0   DOWN
                                Adapter1   UP    00:14:5E:28:27:17
                                Adapter2   UP    00:0E:0C:9C:21:C2
...
```

ステップ 4　ネットワーク インターフェイスにプライオリティの低いハートビート リンクを設定した場合は、プライマリ サーバのクラスタ通信に使用される 2 本目の専用イーサネット ポートからイーサネット ケーブルを取り外します。

ステップ 5　次のコマンドを発行して、すべてのシステムが GAB を介して通信していることを確認します。各サーバではハートビートが 1 つだけ動作しているため、クラスタ内の両方のサーバが Jeopardy 状態になったことも確認します。

```
# gabconfig -a
GAB Port Memberships
===============================================================
Port a gen   e8cc02 membership 01
Port a gen   e8cc02   jeopardy ;1
Port h gen   e8cc01 membership 01
Port h gen   e8cc01   jeopardy ;1
```

ステップ 6　次のコマンドを発行して、クラスタ通信に使用されるリンクの詳細なステータスを表示し、プライマリ サーバ上のクラスタ通信に使用される 2 つ目の専用イーサネット ポートがダウンしていることを確認します。

```
# lltstat -nvv
LLT node information:
    Node           State    Link  Status  Address
   * 0 <PrimaryServer>   OPEN
                                Adapter0   UP    00:14:5E:28:52:9C
                                Adapter1   UP    00:14:5E:28:52:9D
                                Adapter2   UP    00:0E:0C:9C:20:FE
     1 <SecondaryServer> OPEN
                                Adapter0   DOWN
                                Adapter1   UP    00:14:5E:28:27:17
                                Adapter2   DOWN
```

ステップ 7　プライマリ サーバでクラスタ通信に使用される 2 つ目の専用イーサネット ポートのイーサネット ケーブルを交換します。

ステップ 8　次のコマンドを発行して、Jeopardy 状態が解消されたことを確認します。

```
# gabconfig -a
GAB Port Memberships
===============================================================
Port a gen   e8cc02 membership 01
Port h gen   e8cc01 membership 01
```

ステップ 9　プライマリ サーバでクラスタ通信に使用される最初の専用イーサネット ポートのイーサネット ケーブルを交換します。

サーバの障害

ここでは、サーバから電源を取り外してサーバ障害を引き起こします。4 つのケースについて説明します。

- 「スタンバイ サーバの障害、シングル クラスタ」（P.B-10）
- 「プライマリ サーバの障害、シングル クラスタ」（P.B-11）
- 「スタンバイ サーバの障害、デュアル クラスタ」（P.B-12）
- 「プライマリ サーバの障害、デュアル クラスタ」（P.B-14）

スタンバイ サーバの障害、シングル クラスタ

テスト ケース タイトル：シングル クラスタ構成のスタンバイ サーバで障害が発生しました。

説明：このテスト ケースでは、プライマリ サーバで稼働しているアプリケーションが影響を受けないことと、スタンバイ サーバが修復された後、アプリケーションが正常にクラスタ構成に再度参加できることを確認します。

テスト セットアップ：2 本の専用クラスタ通信イーサネット接続、およびネットワーク イーサネット接続のプライオリティの低いクラスタ通信接続を備えた、デュアル ノード クラスタ（図 2-2（P.23））。

ステップ 1　アプリケーションがクラスタ内のプライマリ サーバで実行されていることを確認します。

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               ONLINE
B  APP             <SecondaryServer>    Y          N               OFFLINE
```

ステップ 2　セカンダリ サーバの電源を取り外し、VCS が障害を検出し、アプリケーションがプライマリ サーバで実行し続けることを確認します。

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0
A  <SecondaryServer>    FAULTED              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               ONLINE
```

ステップ 3　電源を再度適用し、セカンダリ サーバをブートします。サーバが回復したら、次のコマンドを実行して、正常な状態でクラスタに再接続されていることを確認します。出力はステップ 1 の出力と同一である必要があります。

```
C:\> hastatus -sum
```

プライマリ サーバの障害、シングル クラスタ

テスト ケース タイトル: シングル クラスタ内のプライマリ サーバで障害が発生しました。

説明: このテスト ケースでは、プライマリ サーバで障害が発生するとセカンダリ サーバでアプリケーションが実行を開始することと、プライマリ サーバが修復された後、アプリケーションをプライマリ サーバで再設定できることを確認します。

テスト セットアップ: デュアル ノード クラスタ（図 1-1（P.12））。

ステップ 1　次のコマンドの出力を調べて、APP サービス グループがクラスタ内のプライマリ サーバで実行されていることを確認します。

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               ONLINE
B  APP             <SecondaryServer>    Y          N               OFFLINE
```

ステップ 2　プライマリ サーバの電源を取り外し、VCS が障害を検出し、APP サービス グループがセカンダリ サーバに正常に移行されることを確認します。

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      FAULTED              0
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <SecondaryServer>    Y          N               ONLINE
```

ステップ 3　クライアント マシンから Security Manager に正常にログインできることを確認します。

ステップ 4　電源をプライマリ サーバに復元し、サーバが正常な状態でクラスタに再参加できることを確認します。次のコマンドを実行します。出力はステップ 1 の出力と同一である必要があります。

```
C:\> hastatus -sum
```

ステップ 5　APP サービス グループを再びプライマリ サーバに手動で切り替えます。

```
C:\> hagrp -switch APP -to primary_server_name
```

スタンバイ サーバの障害、デュアル クラスタ

テスト ケース タイトル: デュアル クラスタ構成のスタンバイ サーバで障害が発生しました。

説明: このテスト ケースでは、プライマリ クラスタで稼働しているアプリケーションがスタンバイ サーバの障害の影響を受けないことと、スタンバイ サーバが修復された後、アプリケーションが正常にデュアル クラスタ構成に再度参加できることを確認します。

テスト セットアップ: 各クラスタ内に複製が行われる 1 台のノードが配置されたデュアル クラスタ構成（図 1-2（P.14））。

ステップ 1　プライマリ サーバで次のコマンドを実行して、APP および ClusterService サービス グループがプライマリ クラスタで動作していることを確認します。

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               ONLINE
B  APPrep          <PrimaryServer>      Y          N               ONLINE
B  ClusterService  <PrimaryServer>      Y          N               ONLINE

-- WAN HEARTBEAT STATE
-- Heartbeat       To                   State
L  Icmp            csm_secondary        ALIVE

-- REMOTE CLUSTER STATE
-- Cluster         State
M  csm_secondary   RUNNING

-- REMOTE SYSTEM STATE
-- cluster:system                  State                Frozen
N  csm_secondary:<SecondaryServer> RUNNING              0

-- REMOTE GROUP STATE
-- Group           cluster:system                  Probed     AutoDisabled    State
O  APP             csm_secondary:<SecondaryServer> Y          N               OFFLINE
```

ステップ 2　電源をセカンダリ サーバから取り外し、プライマリ クラスタがセカンダリ クラスタとの通信の喪失を検出することを確認します。

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               ONLINE
B  APPrep          <PrimaryServer>      Y          N               ONLINE
B  ClusterService  <PrimaryServer>      Y          N               ONLINE

-- WAN HEARTBEAT STATE
-- Heartbeat       To                   State
L  Icmp            csm_secondary        ALIVE

-- REMOTE CLUSTER STATE
-- Cluster         State
M  csm_secondary   LOST_CONN

-- REMOTE SYSTEM STATE
-- cluster:system                  State                Frozen
N  csm_secondary:<SecondaryServer> RUNNING              0

-- REMOTE GROUP STATE
-- Group           cluster:system                  Probed     AutoDisabled    State
O  APP             csm_secondary:<SecondaryServer> Y          N               OFFLINE
```

ステップ 3　セカンダリ サーバに電源を戻します。サーバの再起動後、プライマリ クラスタで次のコマンドを実行して、セカンダリ クラスタとの通信を再確立したことを確認します。出力はステップ 1 の出力と同一である必要があります。

```
C:\> hastatus -sum
```

ステップ 4　次のコマンドを実行して、複製が機能し、矛盾していないことを確認します。

```
C:\> vxprint -Pl
Diskgroup = BasicGroup

Diskgroup = datadg

Rlink      : rlk_172_6037
info       : timeout=16 packet_size=1400
             latency_high_mark=10000 latency_low_mark=9950
             bandwidth_limit=none
state      : state=ACTIVE
             synchronous=off latencyprot=off srlprot=off
assoc      : rvg=CSM_RVG
             remote_host=172.25.84.34
             remote_dg=datadg
             remote_rlink=rlk_172_32481
             local_host=172.25.84.33
protocol   : UDP/IP
flags      : write attached consistent connected
```

プライマリ サーバの障害、デュアル クラスタ

テスト ケース タイトル：デュアル クラスタ構成のプライマリ サーバで障害が発生しました。

説明：このテスト ケースでは、プライマリ サーバで障害が発生するとセカンダリ サーバでアプリケーションが実行を開始することと、プライマリ サーバが修復された後、アプリケーションをプライマリ サーバで再設定できることを確認します。

テスト セットアップ：各クラスタ内に複製が行われる 1 台のノードが配置されたデュアル クラスタ構成（図 1-2（P.14））。

ステップ 1　セカンダリ サーバから次のコマンドを実行して、APP および ClusterService サービス グループがプライマリ クラスタで動作していることを確認します。

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <SecondaryServer>    Y          N               OFFLINE
B  APPrep          <SecondaryServer>    Y          N               ONLINE
B  ClusterService  <SecondaryServer>    Y          N               ONLINE

-- WAN HEARTBEAT STATE
-- Heartbeat       To                   State
L  Icmp            csm_primary          ALIVE

-- REMOTE CLUSTER STATE
-- Cluster         State
M  csm_primary     RUNNING

-- REMOTE SYSTEM STATE
-- cluster:system       State                Frozen
N  csm_primary:<PrimaryServer> RUNNING              0

-- REMOTE GROUP STATE
-- Group           cluster:system              Probed     AutoDisabled    State
O  APP             csm_primary:<PrimaryServer> Y          N               ONLINE
```

ステップ 2　プライマリ サーバから電源を取り外してサーバ障害を引き起こします。セカンダリ クラスタがプライマリ クラスタへの接続の喪失を報告したことを確認します。

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <SecondaryServer>    Y          N               OFFLINE
B  APPrep          <SecondaryServer>    Y          N               ONLINE
B  ClusterService  <SecondaryServer>    Y          N               ONLINE

-- WAN HEARTBEAT STATE
-- Heartbeat       To                   State
L  Icmp            csm_primary          ALIVE

-- REMOTE CLUSTER STATE
-- Cluster         State
M  csm_primary     LOST_CONN
```

```
-- REMOTE SYSTEM STATE
-- cluster:system              State                Frozen
N  csm_primary:<PrimaryServer> RUNNING              0

-- REMOTE GROUP STATE
-- Group           cluster:system              Probed     AutoDisabled    State
O  APP             csm_primary:<PrimaryServer> Y          N               ONLINE
```

ステップ 3　複製の状態が disconnected であることを確認します。次のコマンド出力の **flags** パラメータからこの状態を確認できます。

```
C:\> vxprint -Pl
Diskgroup = BasicGroup

Diskgroup = datadg

Rlink      : rlk_172_32481
info       : timeout=500 packet_size=1400
             latency_high_mark=10000 latency_low_mark=9950
             bandwidth_limit=none
state      : state=ACTIVE
             synchronous=off latencyprot=off srlprot=off
assoc      : rvg=CSM_RVG
             remote_host=172.25.84.33
             remote_dg=datadg
             remote_rlink=rlk_172_6037
             local_host=172.25.84.34
protocol   : UDP/IP
flags      : write attached consistent disconnected
```

ステップ 4　次のコマンドを使用してセカンダリ サーバでアプリケーションを起動します。

```
C:\> hagrp -online -force APP -sys secondary_server_name
```

ステップ 5　アプリケーションにログインし、プライマリ サーバに戻っても、アプリケーションがセカンダリ サーバ上で稼働している間に行われた変更を保持できることを後で確認できるように、データを変更します。

ステップ 6　電源をプライマリ サーバに戻し、サーバが完全に起動できるようにします。

ステップ 7　複製が connected であることを示す複製のステータスを確認します。ただし、両側が同期していません。

```
C:\> vxprint -Pl
Diskgroup = BasicGroup

Diskgroup = datadg

Rlink      : rlk_172_32481
info       : timeout=500 packet_size=1400
             latency_high_mark=10000 latency_low_mark=9950
             bandwidth_limit=none
state      : state=ACTIVE
             synchronous=off latencyprot=off srlprot=off
assoc      : rvg=CSM_RVG
             remote_host=172.25.84.33
             remote_dg=datadg
             remote_rlink=rlk_172_6037
             local_host=172.25.84.34
protocol   : UDP/IP
flags      : write attached consistent connected dcm_logging failback_logging
```

ステップ 8　元のプライマリ RVG をセカンダリに変換し、高速フェールバック機能を使用して、元のプライマリ RVG のデータ ボリュームを新しいプライマリ RVG のデータ ボリュームと同期します。セカンダリ クラスタの Cluster Explorer を使用して、RVGPrimary リソース（**APP_RVGPrimary**）を右クリックし、[actions] を選択して [Actions] ダイアログボックスから [fbsync] を選択し、[OK] をクリックします。または、次のコマンドを発行できます。

```
C:\> hares -action APP_RVGPrimary fbsync 0 -sys secondary_server_name
```

ステップ 9　次のコマンド出力の **flags** パラメータの **consistent** キーワードを調べて、現在のセカンダリ（以前のプライマリ）が現在のプライマリ（以前のセカンダリ）と同期していることを確認します。

```
C:\> vxprint -Pl
Diskgroup = BasicGroup

Diskgroup = datadg

Rlink      : rlk_172_32481
info       : timeout=29 packet_size=1400
             latency_high_mark=10000 latency_low_mark=9950
             bandwidth_limit=none
state      : state=ACTIVE
             synchronous=off latencyprot=off srlprot=off
assoc      : rvg=CSM_RVG
             remote_host=172.25.84.33
             remote_dg=datadg
             remote_rlink=rlk_172_6037
             local_host=172.25.84.34
protocol   : UDP/IP
flags      : write attached consistent connected
```

ステップ 10　セカンダリ クラスタで VCS Cluster Explorer を使用して、[APP] サービス グループを選択します。ショートカット メニューから、[Switch To]、[Remote Switch(...)] の順に選択して [Switch global] ダイアログボックスを開きます。ダイアログボックスで、プライマリ クラスタとプライマリ サーバを指定します。または、次のコマンドを発行します。*primarycluster* はプライマリ クラスタの名前です。

```
C:\> hagrp -switch APP -any -clus primarycluster
```

ステップ 11　アプリケーションにログインして、セカンダリ サーバに加えた変更が保持されていることを確認します。

アプリケーションの障害

ここでは、Security Manager アプリケーションで障害が発生した場合のテスト ケースについて説明します。シングル クラスタ構成とデュアル クラスタ構成の 2 つのケースについて説明します。ここでは、次の項目について説明します。

- 「アプリケーションの障害、シングル クラスタ」（P.B-16）
- 「アプリケーションの障害、デュアル クラスタ」（P.B-17）

アプリケーションの障害、シングル クラスタ

テスト ケース タイトル：シングル クラスタ構成内のプライマリ サーバでアプリケーションの障害が発生しました。

説明: このテスト ケースでは、VCS がアプリケーションの障害を検出し、アプリケーションを自動的にセカンダリ サーバに移行することを確認します。

テスト セットアップ: デフォルトのアプリケーション フェールオーバー動作を使用するデュアル ノード クラスタ（図 1-1（P.12））。

ステップ 1　次のコマンドを実行して、APP サービス グループがクラスタ内のプライマリ サーバで実行されていることを確認します。

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A <PrimaryServer>       RUNNING              0
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               ONLINE
B  APP             <SecondaryServer>    Y          N               OFFLINE
```

ステップ 2　Security Manager が実行されているサーバで、次のコマンドを発行してアプリケーションを停止します。

```
C:\> net stop crmdmgtd
```

ステップ 3　VCS がプライマリ サーバで Security Manager が失敗したことを検出し、アプリケーションをセカンダリ サーバで開始することを確認します。

```
# hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               OFFLINE|FAULTED
B  APP             <SecondaryServer>    Y          N               ONLINE

-- RESOURCES FAILED
-- Group           Type                 Resource             System
C  APP             CSManager            APP_CSManager        <PrimaryServer>
```

ステップ 4　APP サービス グループの障害を手動で解決します。

```
C:\> hagrp -clear APP -sys primary_server_name
```

ステップ 5　APP サービス グループを再びプライマリ サーバに手動で切り替えます。

```
C:\> hagrp -switch APP -to primary_server_name
```

アプリケーションの障害、デュアル クラスタ

テスト ケース タイトル: デュアル クラスタ構成内のプライマリ サーバでアプリケーションの障害が発生しました。

説明: このテスト ケースでは、VCS がアプリケーションの障害を検出することを確認します。

テスト セットアップ: 各クラスタ内に複製が行われる 1 台のノードが配置されたデュアル クラスタ構成（図 1-2（P.14））。同様に、デフォルトのアプリケーション フェールオーバー動作が変更されていない（つまり、クラスタ間のフェールオーバーに手動による介入が必要である）ことを前提とします。

ステップ 1　プライマリ サーバで次のコマンドを実行して、APP および ClusterService サービス グループがプライマリ クラスタで動作していることを確認します。

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <SecondaryServer>    Y          N               OFFLINE
B  APPrep          <SecondaryServer>    Y          N               ONLINE
B  ClusterService  <SecondaryServer>    Y          N               ONLINE

-- WAN HEARTBEAT STATE
-- Heartbeat       To                   State
L  Icmp            csm_primary          ALIVE

-- REMOTE CLUSTER STATE
-- Cluster         State
M  csm_primary     RUNNING

-- REMOTE SYSTEM STATE
-- cluster:system       State                Frozen
N  csm_primary:<PrimaryServer> RUNNING              0

-- REMOTE GROUP STATE
-- Group           cluster:system              Probed     AutoDisabled    State
O  APP             csm_primary:<PrimaryServer> Y          N               ONLINE
```

ステップ 2　Security Manager が実行されているサーバで、次のコマンドを発行してアプリケーションを停止します。

```
C:\> net stop crmdmgtd
```

ステップ 3　VCS がアプリケーションの障害を検出し、APP サービス グループを停止したことを確認します。次のコマンドを発行し、出力を確認します。

```
# hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               OFFLINE|FAULTED
B  APPrep          <PrimaryServer>      Y          N               ONLINE
B  ClusterService  <PrimaryServer>      Y          N               ONLINE

-- RESOURCES FAILED
-- Group           Type                 Resource             System
C  APP             CSManager            APP_CSManager        <PrimaryServer>

-- WAN HEARTBEAT STATE
-- Heartbeat       To                   State
L  Icmp            csm_secondary        ALIVE

-- REMOTE CLUSTER STATE
```

```
-- Cluster         State
M  csm_secondary   RUNNING

-- REMOTE SYSTEM STATE
-- cluster:system                  State                Frozen
N  csm_secondary:<SecondaryServer> RUNNING              0

-- REMOTE GROUP STATE
-- Group           cluster:system                  Probed     AutoDisabled    State
O  APP             csm_secondary:<SecondaryServer> Y          N               OFFLINE
```

ステップ 4　APP サービス グループの障害を手動で解決します。

```
C:\> hagrp -clear APP
```

ステップ 5　APP サービス グループをプライマリ サーバでオンラインにしてアプリケーションを再起動します。

```
C:\> hagrp -online APP -sys primary_server_name
```

INDEX

A

ACS
- Security Manager との統合 4-6

M

Microsoft Windows
- インストール 3-2

S

Security Manager
- アップグレード 4-6
- アンインストール 4-7
- インストールの概要 3-6
- 手動での起動、停止、またはフェールオーバー 4-3
- セカンダリ サーバへのインストール 3-9
- バックアップ 4-7
- プライマリ サーバへのインストール 3-7

Symantec Veritas
- 「Veritas」を参照 3-2

V

Veritas Cluster Server
- 設定、シングル ローカル クラスタ（デュアル ノード） 3-16
- 設定、デュアル地理的クラスタ 3-25
- 動作のカスタマイズ 4-1
- リソース ビュー A-1

Veritas Volume Manager
- セカンダリ サーバの設定 3-6
- プライマリ サーバの設定（複製あり） 3-5
- プライマリ サーバの設定（複製なし） 3-4

Veritas Volume Replicator
- 設定 3-12

Veritas 製品
- インストール 3-2
- 概要 1-5

い

イーサネット接続
- 確立 3-1

か

外部ストレージ
- サーバに接続 3-2

概要 1-1

け

警告
- 重要 ix

権限
- 作業ボリュームに対する更新 3-14

さ

サポート
- 取得 x

し

システム要件
概要 2-1
ソフトウェア、クラスタリングが不要な複製 2-4
ソフトウェア、地理的冗長性 2-4
ソフトウェア、ローカル冗長性 2-3
ハードウェア、シングル ノード サイト 2-1
ハードウェア、デュアル ノード サイト 2-2

せ

セキュリティ ガイドライン
取得 x

ち

注意
重要 ix

て

テスト計画
アプリケーションの障害 B-16
イーサネット / ネットワーク障害 B-3
サーバの障害 B-10
手動切り替え B-1

ひ

表記法 viii

ふ

ブート ディスク
ミラーリング 3-3

ま

マニュアル
関連資料 ix
順序 x
対象読者 vii
表記法 viii

わ

ワークシート
地理的冗長性 2-6
ローカル冗長性 2-5

©2008 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。
「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)
この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/